NAME: 'MAMOTUMI MALIEHE

STUDENT NUMBER: MLHMAM002

QUALIFICATION: LLM ELECTRONIC LAW

DISSERTATION TITLE: CYBERCRIME LEGISLATION FOR LESOTHO

SUPERVISOR: ASSOCIATE PROFESSOR JULIEN HOFMAN

DATE: FEBRUARY 2007

Research dissertation presented for the approval of Senate in fulfilment of part of the requirements for the LLM Electronic Law in approved courses and a minor dissertation. The other part of the requirement for this qualification was the completion of a programme of courses.

I hereby declare that I have read and understood the regulations governing the submission of LLM Electronic Law dissertations, including those relating to length and plagiarism, as contained in the rules of this University, and that this dissertation conforms to those regulations.

PLAGIARISM DECLARATION

1. I know that plagiarism is wrong. Plagiarism is to use another's work and pretend that it is one's own.

2. I have used the **Chicago Style** for citation and referencing. Each contribution to, and quotation in, this thesis from the work(s) of other people has been attributed, and has been cited and referenced.

3. This thesis is my own work.

4. I have not allowed, and will not allow, anyone to copy my work with the intention of passing it off as his or her own work.

Signature _____

Date _____

ABSTRACT

This paper advocates introducing cybercrime legislation in Lesotho. Cybercrime is the hottest issue today. Cybercriminals can commit various illegal activities in cyberspace that few people even know exist. A nightmare scenario would be a hacker breaking into the hospital's computer systems on a fine morning and before doctors can arrive to treat their patients, the malicious hacker modifies patients' files on the hospital's database systems:

> [S]urgeries slated to be performed on the right leg are now switched to the left leg; recorded blood types are altered from AB-negative to O-positive; warnings for known allergies to medicines such as penicillin are electronically erased from patients' charts; and laboratory records on HIV blood tests results are insidiously switched from negative to positive just before patients are to receive their results. (Marc D Goodman 'Why the police don't care about computer crime' (1997) 10 *Harvard Journal of Law and Technology* 465 at 466).

Although this scenario is possible with current technology, unfortunately Lesotho would be powerless to act for lack of adequate laws to investigate and prosecute this conduct. Lesotho's current criminal laws can hardly be enforced against cybercrime, as they do not clearly prohibit the crime. Therefore, this paper argues that Lesotho must adopt a comprehensive legal structure to deter and prosecute cybercrime. It does this by examining international and national approaches to cybercrime, with a view to providing guidance for an effective framework capable of addressing this 'new' crime. Cybercrime is a major global challenge requiring coordinated international effort. In a networked world no island is an island; cybercrime penetrates all countries because of its ability to cross national boundaries. Further, this paper suggests a model law that is based on the first international treaty which plays a key role in combating cybercrime. Finally, it recognises that legislation alone cannot fight cybercrime; law enforcement must be equipped to implement the law, and private citizens must know about cybercrime and the need to protect themselves and their systems and networks.

DEDICATION

For Ntaote Bereng and Kananelo Bontle Maliehe

This study is dedicated to Ntaote Bereng for the wonderful gifts: providing me with purpose and initiating my curiosity in exploring electronic law; and to my daughter, Kananelo Bontle Maliehe for making it worthwhile, and for always telling me that if I didn't read I would fail.

ACKNOWLEDGEMENTS

This work is the result of extensive research in the field of Electronic Law. I would never have survived the research period, let alone produced this work, had it not been for the purpose which Ntaote Bereng provided, and the wonderful support and friendship of many people. In no particular order, I would like to thank these people:

My supervisor, Associate Professor Julien Hofman, for the insightful comments and valuable supervision throughout, steering me in the right direction, enriching my mind, and broadening my horizons.

Linda van de Vijver, for accommodating me at the last minute and tirelessly checking and proofreading my work - and she is very smart.

Doris and Dorothy, in the Faculty of Law at the University of Cape Town, for opening their doors and hearts to me; their smiles kept me going.

Davis Luthe, for helping me to understand better the practical use of ‘conjunctions’ without which this paper would truly be rough around the edges. Additionally, I appreciate his devoted time and wise interventions.

Moeketsi D. Palime, a colleague, and Thenjiswa Matshikiza, a friend, for providing valuable information when I needed it most.

Nkoya M .G. Thabane, a fine friend and lawyer, for providing wisdom, information and for so many other forms of support when I needed them most.

Cecilia M. Petlane, for the back-up system; being a great ‘adoptive sister’ and a terrific ‘mother’ to ‘my kids’, making this work possible and providing good humour at the most difficult of times. She absolutely blessed this work in so many ways.

Sellone ‘Mapuleng Thorela, for always encouraging me and helping me to keep things in perspective.

Malikhoa Chonela and her family, for taking time out for me when I needed it most, which feels good, hey!

Thotoane Ramlefane, for redefining the meaning of friendship, and actually going beyond the call of friendship; knowing that I could always count on her made everything possible and easier.

Likonelo Lebone, for providing moral and other practical support.

Princess Anne Keneuoe Maliehe, for facilitating to get me into the very finest teaching and research university, at the eleventh hour.

Ellen Paballo Maliehe, for enduring my frustrations and perhaps understanding the pressure that goes with taking care of two kids of different ages; sometimes behaving as if they are the same age. Further, I appreciate her helping hand.

My precious family, particularly Nkhono Thabie and my parents, for providing emotional support, practical assistance, and, most important, love.

The Lesotho Ministry of Law and Constitutional Affairs (particularly, the Registrar General’s Office) for providing me the opportunity to further my studies and the Government for sponsoring me.

I am solely responsible for this work and happy to be so.

TABLE OF CONTENTS

LIST OF FIGURES

CHAPTER ONE: DEFINING CYBERCRIME

1. Introduction

The rapidly growing danger from criminal activities committed on the Internet, broadly defined as cybercrime, is beginning to claim attention in many national governments.[1] In Lesotho, however, current criminal laws can hardly be enforced against cybercrime. Cybercrime is a new phenomenon and Lesotho has not enacted laws to combat it. This absence of legal protection means that businesses and society must resort to technical measures to protect themselves against cybercrime.[2] Although self-protection is essential, it is not enough to fight cybercrime and to make Lesotho a safe place to conduct business.[3] Criminals have discovered that the Internet provides excellent opportunities and benefits for illicit business and other criminal activities at a minimal risk.[4] 'When the Internet was developed, the founding fathers of the Internet hardly had any inclination that the Internet could also be misused for criminal activities. Today, there are many disturbing things happening in cyberspace.'[5] Obviously, '[i]t was just a matter of time before criminals discovered the advantages of computers … computers make it increasingly possible to get proprietary information of financial institutions and other firms.'[6] Indeed, Lesotho can prosecute some types of this illegal activity (such as forgery and fraud) using current criminal laws, but some activities (such as hacking and the dissemination of computer viruses) cannot be covered by existing laws.

---

[1] See McConnell International 'Cybercrime…punishment? archaic laws threaten global information' (December 2000). Available at http://www.mcconnellinternational.com/services/cybercrime.htm [Accessed 20 June 2006].
[2] See ibid.
[3] See ibid. McConnell International's argument does not specifically address Lesotho; it generally refers to all those countries unable to prosecute cybercrime.
[4] See Phil Williams 'Organized crime and cybercrime: synergies, trends, and responses' (13 August 2001). Available at http://usinfo.state.gov/journals/itgic/0801/ijge/gj07.htm [Accessed 4 July 2006].
[5] Shri Pavan Duggal 'Cyber assault & cybercrimes.' Available at http://cyberlaws.net/cyberindia/cyberassault.htm [Accessed 11 April 2006].
[6] Glenn D Baker 'Trespassers will be prosecuted: computer crime in the 1990s' (1993) 12 *Computer/Law Journal* 61at 62.

Lesotho is part of the world now run by all electrons; 'ones and zeros… little bits of data', with information technologies affecting virtually every aspect of business and society.[7] While the Internet is a great communications tool for ordinary law-abiding citizens, at the same time, it is a powerful and dangerous tool for criminals; criminals use the internet as an ideal channel and instrument for many criminal activities.[8] Therefore, Lesotho must ensure that it preserves mankind's growing wealth and military power being stored and channelled on the Internet by enforcing the rule of law.

Cybercrime creates significant law enforcement challenges for Lesotho. Generally, sophisticated Internet criminals are aware of the anonymity the Internet offers, and the difficulties that law enforcement encounters in piercing this veil.[9] As a result, these criminals adjust their activities to maximise their anonymity on the Internet.[10] In response to the misuse of computer systems and networks, Lesotho must criminalise specific conduct, and create civil or private rights to ensure creating enforcement of violations of protected rights. Lesotho must draw on best practices from other countries and work closely with the industry to enact enforceable legal protections against cybercrime.[11]

1.1 Challenges facing Lesotho

Lesotho's criminal laws are based on the common law and the statutes.[12] Lesotho's traditional classification of existing common law and statutory crimes does not cater for the prosecution of cybercrime. The existing criminal laws against trespass or

---

[7] See Marc D Goodman 'Why the police don't care about computer crime' (1997) 10 *Harvard Journal of Law and Technology* 465 at 466. See also the Remarks of James K Robinson 'Internet as the scene of crime' International computer crime conference (29-31 May 2000). Available at http://www.usdoj.gov/criminal/cybercrime/roboslo.htm [Accessed 20 June 2006]. The Internet penetrates the whole world.

[8] See Williams note 4.

[9] See Joel Michael Schwarz 'A case of identity: a gaping hole in the chain of evidence of cyber-crime' (2003) 9 *Boston University Journal of Science and Technology Law* 92 at 93.

[10] See ibid.

[11] See McConnell International note 1. McConnell International suggests that all countries must be able to prosecute cybercrime.

[12] Lesotho's common law is a mixture of Roman-Dutch law and some English law. See Sebastian Poulter *Legal dualism in Lesotho* (1979) 3-4. See also 'The World Factbook.' Available at www.cia.gov/cia/publications/factbook/print/lt.html [Accessed 12 January 2007].

breaking and entering are ill-suited to their 'virtual' counterparts. For instance, charging a hacker with the traditional crime of house-breaking would be difficult because a computer cannot amount to 'premises,' a required element in house-breaking. Similarly, the Distributed Denial of Service attacks cannot be prosecuted with the common-law crime of malicious damage to property because information is not tangible enough to be regarded as physical 'property', a required element for malicious damage to property. Thus, for example, Lesotho's laws cannot cover web pages like the e-commerce sites, Yahoo, CNN, and E-Bay that were hit by widespread, distributed denial of service attacks, as protected forms of property.[13]

Cybercrime yields various 'new' forms of criminal activities that current laws do not cover, as the Philippines learned when attempting to prosecute the author of the May 2000 'Love Bug' virus which spread worldwide, causing tremendous financial damage.[14] 'Since the Philippines had no cybercrime laws, creating and distributing the virus was not a crime', and as a result, the perpetrator had to be released without being charged, despite the gravity of his act.[15] Although some of the countries affected, such as the United States, have laws to prosecute the offence, extradition was impossible for the lack of any extradition treaty between the countries.[16] Furthermore, to execute such a treaty the relevant offence has to be criminal according to the laws of every country involved.[17] Nevertheless, six weeks later the Philippines adopted cybercrime legislation and a few other countries have also followed suit.[18]

---

[13] In February 2000, some Internet sites (among others Yahoo, CNN and E-Bay) were temporarily crippled by a malicious computer attack, 'Denial of Service Attacks', which shut them down. See Robinson note 7.

[14] McConnell International note 1.

[15] See, for example, Marc D Goodman and Susan W Brenner 'The emerging consensus on criminal conduct in cyberspace' (2002) 3 *UCLA Journal of Law and Technology*. See also Susan W Brenner 'Cybercrime investigation and prosecution: the role of penal and procedural law' (2001) vol. 8(2) *Murdoch University Electronic Journal of Law.* Available at http://www.murdoch.edu.au/elaw/indices/issue/v8n2.html [Accessed 25 January 2007].

[16] See, for example, Abraham A Purugganan 'Philippines cybersecurity update: laws cases & other legal issues in Pauline C Reich (ed) *Cybercrime and security* (2006) 9. See also Lynn Burke 'Love bug case dead in Manila' Wired News (21 August 2000). Available at http://www.wired.com/news/politics/0,38342-1.html?tw=wn_story_page_next1,00.html [Accessed 18 January 2007].

[17] See ibid.

[18] See, for example, McConnell note 1. See also Brenner note 15.

Cybercrime poses far greater challenges to law enforcement because of its ability to evade the reach of the existing criminal laws.[19] Challenges facing Lesotho can generally be divided into three categories:

- Technical challenges hindering law enforcement's ability to trace and prosecute criminals operating online;

- Legal challenges resulting from the fact that the laws and legal tools needed to investigate cybercrime lag behind technological structures and social changes; and

- Operational challenges ensuring the creation of a network of well-trained, well-equipped investigators and prosecutors working together with unprecedented speed even across national borders.[20]

1.1.1 Technical challenges

When a cybercrime occurs online, law enforcement must identify the person responsible; and to accomplish this, law enforcement must trace the crime from the victim back to the perpetrator. But herein lies the rub, '[t]racing a criminal in the electronic age, however, can be difficult, especially if we require international cooperation, if the perpetrator attempts to hide his identity, or if technology otherwise hinders our investigation.'[21]

In the virtual world borders do not exist, and this is an attractive characteristic for criminal activity.[22] The inherent transnational nature of the Internet provides an added degree of protection against law enforcement and allows criminals to operate with minimal risk.[23] Criminals can weave their communications through service providers in various countries to cover their tracks, thus creating added complexities

[19] See Goodman note 15. See also Williams note 4.
[20] See Robinson note 7.
[21] Ibid.
[22] See Williams note 4.
[23] See ibid.

to governments trying to find criminals.[24] The establishment of mutual legal assistance between governments involves sharing evidence between only two countries, the victim's country and the criminal's country.[25] Unfortunately, however:

> [W]hen a criminal sends his communications through a third, or fourth, or fifth country, the processes for international assistance involve successive periods of time before law enforcement can reach data in those latter countries, increasing the chances the data will be unavailable or lost, and the criminal will remain free to attack again.[26]

To identify and trace global communications, Lesotho must work across borders, not only with her counterparts worldwide, but again with industry, to preserve evidence such as log files, e-mail records, and other files, and Lesotho must be able to do so swiftly, before such communication is altered or deleted.[27] The investigation may falter if information is not obtained quickly.[28] Simultaneously, tracing transmissions has to be done in real time, during an actual communication.[29] However, this can be technically difficult, as many communications technologies do not facilitate tracing.[30] Although less sophisticated cybercriminals may leave electronic 'fingerprints', more experienced criminals can cover their tracks.[31] Tracing cybercriminals becomes difficult and sometimes impossible, particularly when using anonymous software.[32] Cybercriminals can hide their actions behind a veil of anonymity, which ranges from using ubiquitous cybercafes to sophisticated efforts that to cover Internet routing.[33] Other services in other countries, such as pre-paid calling cards, facilitate anonymous communications and all of these technologies make tracing criminals difficult, at best, and impossible, at worst, though these services may have their advantages.[34]

Countless other technical challenges face Lesotho, like those originating from Internet telephony, strong encryption, and wireless and satellite communications.[35]

---

[24] See Robinson note 7.
[25] See ibid.
[26] Ibid.
[27] See ibid.
[28] See ibid.
[29] See ibid.
[30] See ibid.
[31] See ibid.
[32] See ibid.
[33] See Williams note 4.
[34] See Robinson note 7.
[35] See ibid.

The technological advances in electronic commerce and communication that have led to the rapid growth of the Internet have also enabled international criminals to victimise people anywhere in the world, in unprecedented ways.[36]

In a sophisticated age of anonymous, wireless, and encrypted communications how is Lesotho to identify and prosecute criminals who are victimising her citizens and businesses?[37] What role does the country play when criminals located domestically use satellite and wireless communications, travelling exclusively through gateways located elsewhere?[38]

Though the Internet may be borderless, national boundaries do exist for law enforcement. Therefore, Lesotho must create an environment conducive to finding and prosecuting cybercriminals and must teach the world at large to respect her sovereignty.[39] In particular:

> We increasingly are dependent on mutual cooperation from other countries in investigating and prosecuting computer crimes. Simply stated, cybercrimes know no national boundaries, and the multi-jurisdictional nature of cybercrimes require a new multilateral approach to investigations and prosecutions.[40]

1.1.2 Legal challenges

The inherent transnational nature of the Internet, 'rendering the traditional concept of distance meaningless', allows criminals to act with impunity.[41] They act with impunity because they are not afraid of justice. 'Undeterred by the prospect of arrest or prosecution, cybercriminals around the world lurk on the Net as an omnipresent menace to the financial health of businesses, to the trust of their customers, and as an emerging threat to the nations' security.'[42] Lesotho must deal with cybercrime seriously. These criminal activities must not be considered mere pranks, but injuries with serious security and/or financial implications.

---

[36] See ibid.
[37] See ibid.
[38] See ibid.
[39] See ibid.
[40] Ibid.
[41] Goodman (note 7) at 471.
[42] McConnell International note 1.

Indubitably, cybercrime has become a serious threat to our nations.[43] More seriously, it has become the 'weapon of choice' among white-collar criminals, similar to 'any form of theft, except that it's more subtle and it's more sophisticated.'[44]

Deterring and punishing cybercrime requires a legal structure capable of supporting the detection and successful prosecution of criminals.[45] Experiences around the world have shown that a well defined rule of law that strongly deters cybercrime is critical to the effective protection of valuable information and networks.[46] According to the McConnell International survey:

> Outdated laws and regulations, weak enforcement mechanisms for protecting networked information, create an inhospitable environment in which to conduct e-business within a country and across national boundaries. Inadequate legal protection of digital information can create barriers to its exchange and stunt the growth of e-commerce. As e-business expands globally, the need for strong and consistent means to protect networked information will grow.[47]

Since crime is an offence against the authority of the state, Lesotho must assume the responsibility of protecting her citizens and act accordingly. Lesotho must be concerned with fulfilling her obligations to her citizens, namely, protecting lives, property, and morality, and with ensuring her own survival.[48] Adopting cybercrime legislation is necessary in Lesotho, to create a healthy electronic commerce environment. As the United States Justice Department notes,'[l]eft unchallenged computer crime poses a serious threat to the health and safety of our citizens, and may stifle the Internet's power as a tool to communicate, engage in commerce, expand people's educational opportunities around the globe.'[49] To prosecute cybercrime effectively Lesotho needs a clearly defined legal structure, but Lesotho has not adopted any cybercrime legislation. When one country criminalises cybercrime and the other does not, co-operation to prosecute the crime becomes impossible.[50] Indeed,

---

[43] See Baker note 6.
[44] Ibid.
[45] See, for example, Robinson note 7.
[46] See, for example, McConnell International note 7. The most notable example is the Philippines with insufficient laws to prosecute the perpetrator of the 'Love Bug' virus, resulting in great financial damage worldwide.
[47] Note 1.
[48] See Goodman note 15.
[49] CNN.com 'Study: Most nations' laws lag on cybercrime' (6 December 2000). Available at *http://edition.cnn.com/2000/TECH/computing/12/06/crime.tech.reut/index.html* [Accessed 11 April 2006].
[50] See, for example, Robinson note 7. See also Brenner note 15.

inadequate systems for international legal assistance and extradition can prevent the prosecution of criminals, as the 'Love Bug' virus incident taught the investigators.[51] Obviously, Lesotho cannot take any action against cybercriminals before adopting laws that criminalise the activities these criminals engage in:

> National governments should examine their current statutes to determine whether they are sufficient to combat the kinds of crimes in this report [the 'new' cybercrime offences, mostly dealing with information security]. Where gaps exist, governments should draw on best practices from other countries and work closely with the industry to enact enforceable legal protections against these new crimes.[52]

In addition:

> The information infrastructure has significant implications for the governance of an information society. Despite the popular perception, the global information infrastructure (GII) is not a lawless place. Rather, it poses a fundamental challenge for effective leadership and governance. Laws, regulations and standards can, do, and will affect infrastructure development and the behaviour of GII participants. Rules and rule making do exist.[53]

Although cybercrime is a menace to society and Lesotho does not have laws to prosecute it, people may still not even be aware of it. Nevertheless, it is a potential problem.[54] Therefore, individuals and businesses will want to be reassured that the 'Net' will not be used systematically to undermine their security while criminals need to know that the law will not tolerate their criminal misconduct. Additionally, Lesotho needs cybercrime legislation to avoid becoming a home base providing 'safe havens' from which criminals can conduct their transnational operations. 'As cyber crime increasingly breaches national borders, nations perceived as havens run the risk of having their electronic messages blocked by the network.'[55] Further, Lesotho can use cybercrime laws to apprehend and prosecute perpetrators for their explicit acts without relying on outdated laws to cover 'new' offences.[56] Furthermore, Lesotho can

---

[51] See ibid.
[52] McConnell International note 1.
[53] Joel R Reidenberg 'Governing networks and rule-making in cyberspace' (1996) 45 *Emory Law Journal* 911 at 912.
[54] See Goodman (note 7) at 486.
[55] McConnell note 1.
[56] See Stein Schjolberg and Amanda Hubbard 'Harmonizing national legal approaches on cybercrime' at 5. Available at *http://www.itu.int/osg/spu/cybersecurity/docs/Background_Paper_Harmonizing_National_and_Legal_Approaches_on_Cybercrime.pdf* [Accessed 10 June 2006].

also use cybercrime laws to gather evidence for use in courts of law and for establishing precedents and ethical standards more significantly through judgements.[57]

1.1.3 Operational challenges

Cybercrime raises complex technical and legal issues which will require Lesotho to have individuals dedicated to cybercrime and these individuals must have a sound understanding of computers and telecommunications.[58] Technological complexities and the rapidly changing technologies mean that law enforcement must work on cases full-time, immersing themselves in computer-related investigations and prosecutions.[59] Also:

> Given the quickly evolving nature of computer technology, our nations must also continue to increase their computer forensic capabilities, which are so essential in computer crime investigations. Twenty years ago, a new police officer was given a gun, a flashlight, and a notepad. When that officer retired, the three items would be returned to the police department, and the only intervening equipment expenses would have been replacement bullets, batteries, and note paper. Today, keeping pace with computer criminals means that law enforcement experts in this field must be properly equipped with the latest hardware and software.[60]

1.2 Which way Lesotho?

'In a world where no island is an island', Lesotho's failure to address the need for cybercrime legislation may have grave consequences for the rest of the world, as occurred in the Philippines with the 'Love Bug' virus.[61] Equally important, adopting cybercrime legislation would bring Lesotho into consensus with the penal laws adopted by other nations.[62] Additionally, to avoid a repeat of the 'Love Bug' episode and to make the country a safe place in which to conduct business, Lesotho must devise a set of crimes to use to pursue cybercriminals wherever they are operating.[63]

---

[57] See ibid.
[58] See Robinson note 7.
[59] See ibid.
[60] Ibid.
[61] See, for example, Goodman note 15. See also Brenner note 15. Further, see the discussion of the 'Love Bug' virus at 1.1 above and at 2.1.2 below.
[62] See Goodman note 15.
[63] See, for example, Goodman note 15. See also Brenner note 15.

Besides, countries with inadequate legal protections will be less able to compete in the new economy.[64]

However, the difficultly lies in properly defining the laws required to apprehend and prosecute cybercriminals to the fullest extent of the law.[65] Yet, the approach could also be simple; creating an entirely new model for the 'new' offences and modifying the traditional model to accommodate online criminal activity.[66] Just as the human mind is ingenious enough to devise new strategies for committing crimes; so does human ingenuity needs to be channelled into developing effective and regulatory measures of combating cybercrime.

The paper argues that cybercrime legislation is necessary for Lesotho. It begins by examining the nature of cybercrime. To illustrate the extent of cybercrime, the paper then discusses the most common types of the crime, advancing reasons for the adoption of cybercrime legislation. The paper then investigates international and national approaches to combating cybercrime. Next, the paper discusses how Lesotho can make the changes necessary to deter and prosecute criminals using the anonymity of the Internet in criminal activities, and concludes that cybercrime legislation is necessary to combat this 'new' phenomenon. The paper concludes by making some remarks about enacting cybercrime legislation for Lesotho.

2. Definition of cybercrime

Essentially, cybercrime consists of any criminal activity committed from or against a computer or network.[67] The terms 'computer crime,' 'Information Technology crime,' and 'high tech crime' can also be used to refer to this type of criminal behaviour.[68] The crimes committed can be of the conventional straightforward type using new

[64] McConnell International note 1.
[65] See Goodman note 15.
[66] See ibid.
[67] See, for example, Susan W Brenner 'Cybercrime law and policy in the United States' in Pauline C Reich (ed) *Cybercrime and security* (2005) at 1. See also Xan Raskin and Jeannie Schaldach-Paiva 'Eleventh survey of white collar crime' (1996) 33 *American Criminal Law Review* 541 at 542. Further, see Maya Babu 'What is cybercrime?' Available at http://www.crime-research.org/analytics/702 [Accessed 4 October 2006].
[68] See Goodman note 15.

technologies, or they can be new types of crimes committed using highly technical equipment to manipulate and infiltrate computer systems that may be on the other side of the globe.[69]

2.1 The Nature of cybercrime

Cybercrime is global in nature; it knows no national boundaries:

> As networked communications and e-commerce expand around the globe, businesses and consumers become more and more vulnerable to the reach of criminals. The global nature of the Internet enables criminals to hide their identity, commit crimes remotely from anywhere in the world; and to communicate with their confederates internationally. This can happen in nearly any type of crime, from violent crime, terrorism, and drug-trafficking, to the distribution of child pornography and stolen intellectual property, and attacks on e-commerce merchants.[70]

Cybercrimes differ from real-world crimes in four respects:

- they are easy to commit;
- they need few resources compared to the amount of damage potentially caused;
- they can be committed in any jurisdiction without the perpetrator necessarily being at the scene of the crime; and
- they are often not clearly defined as criminal.[71]

The nature of cybercrime can be summed up thus:

> In the networked world, the new generation of vandals and data thugs do not need to have physical contact with the victim. Data is easily copied, transmitted, modified or destroyed. As a result, the scene of crime is a particularly difficult one: there are no fingerprints or traces, identification of the culprits is nearly impossible, apprehension even more so and the legal framework does not make adequate provision for justice in this kind of crime.[72]

---

[69] See, for example, Duggal note 5. See also Goodman note 15. Further, see Brenner note 67.
[70] Robinson note 7.
[71] See McConnell International note 1.
[72] Eduardo Gelbstein and Ahmad Kamal 'Information insecurity' in Pauline C Reich (ed) *Cybercrime and security* (2005) 5

2.1.1 Easy commission

Without ever leaving the comfort of their own homes criminals can victimise individuals and businesses anywhere in the world, with very little risk of apprehension.[73] A criminal merely needs a computer and a modem connected to the Internet to commit a cybercrime. Clearly, conducting a crime is more efficient in cyberspace than in the physical world.[74] A case of identity theft serves as a good example here: the Internet allows the identity thief to obtain personal identifiers of multiple persons more quickly and it also allows them to obtain high-quality fake identification tools (drivers' licences, birth certificates, social security cards, and others).[75] Basically, the 'faceless' nature of e-commerce defeats the purpose of credit-cards, driver's licences and other identification tools.[76] In the offline world of credit purchase transactions, the following prevention and limitation measures can be employed to control identity theft:

- an identity thief can only transact once at a given location and the identity thief needs time to travel to the next location;

- a credit card used by the identity thief has certain security features on the front of the card and on the back in the black strip;

- an identity thief must sign the purchase receipt that must be compared to the signature on the card; and

- an identity thief must be at the scene of the transaction which could lead to physical observation and possible arrest, and this significantly deters many people from attempting to commit this type of crime.[77]

---

[73] See generally Williams note 4. See also Gelbestein ibid.
[74] Gerald R Ferrera, et al *Cyberlaw: text and cases* (2001) 298.
[75] Identity theft occurs when someone uses the identifying information of another person – name, social security number, mother's maiden name, or other personal information – to commit fraud or engage in other unlawful activities. See Social Security Online 'Identity theft.' Available at http://www.ssa.gov/pubs/idtheft.htm [Accessed 4 December 2006].
[76] See Norman A Willox 'Identity theft: authentication as a solution' in Alan E Brill, Fletcher N Baldwin and Robert J Munro (eds) *Cybercrime and Security* (2001) 3.
[77] See ibid 3-4.

Unfortunately, the 'faceless' world of Internet credit purchases does not provide any prevention or limitation measures.[78] The identity thief is at liberty to commit many fraudulent transactions; no physical card or receipt is required; and again the privacy of the Internet offers the identity thief anonymity.[79] At the same time, the Internet offers ample opportunities to commit crimes instantaneously.[80] Additionally, '[t]he Internet is quick, convenient and virtually any amount of information can be sent almost anywhere in the blink of an eye.'[81] For instance, in the physical world when a thief steals credit cards (with or without a Personal Identification Number or PIN), the thief needs time to use these cards, and the owner can report them as lost or stolen before they are used.[82] However, in the networked world when credit card details are stolen, the owner knows nothing about this and the thief who has stolen the person's electronic identification can use this information immediately.[83] Furthermore, in the networked world goods have no weight; therefore, stealing, transferring and storing them become easy.[84]

2.1.2 Few resources vis-à-vis damage

The Internet offers enormous opportunities to commit crimes using limited resources.[85] Armed with computers, computer networks, and related information and communications technologies crimes can easily be committed.[86] Remarkably, a criminal 'can steal more with a computer than with a gun' and 'do more damage with a keyboard than with a bomb.'[87] Perhaps the most notable example is the February 2000 malicious computer attack referred to as the 'Denial of Service Attacks' that temporarily caused major disruptions to the most prominent Internet commerce sites such as Yahoo, CNN, and E-Bay, thereby shutting them down.[88] Another typical example is the distribution of the short-lived, yet destructive 'Love Bug' virus, in May

---

[78] See ibid 4.
[79] See ibid.
[80] See ibid.
[81] Julien Hofman *A guide for South Africans doing business online* (1999) 30.
[82] See Gelbstein (note 72) 5.
[83] See ibid.
[84] See Goodman (note 7) at 472.
[85] See generally Goodman ibid.
[86] See, for example, Goodman note 15.
[87] National Research Council 'Computers at risk' 1991 (quoted in Babu note 67).
[88] See, for example, Robinson note 7. See also note 13.

2000, that affected thousands of corporate websites around the world; many companies had to shut down their e-mails systems to stop the spread of the virus.[89] The effects of the virus have been described as follows:

> The virus destroyed files and stole passwords; it appeared in Hong Kong on May 11, 2000 and spread rapidly throughout the world.
> ….[I]n the offices of the German newspaper Abendblatt in Hamburg, system administrators watched in horror as the virus gobbled up 2,000 digital photographs in the picture archive. In Belgium ATMs were disabled, leaving citizens cashless. In Paris cosmetics maker L'Oreal shut down its e-mail servers, as did other businesses throughout the Continent. As much as 70 % of the computers in Germany, the Netherlands and Sweden were laid low. The companies affected made up a Who's Who of industry and finance, including Ford, Siemens, Silicon Graphics and Fidelity Investments. Even Microsoft … got so badly battered that it finally severed outside e-mail links at its Redmond, Wash., headquarters.
> Governments too, felt the pain. In London, Parliament shut down its servers before the Love Bug's assault ….
> On Capitol Hill, crippled e-mail systems forced an atypical silence in the halls of Congress….
> The Bug infected 80% of all federal agencies, including both the Defense and State departments, leaving them temporarily out of e-mail contact with their far-flung outposts….
> [T]he virus corrupted no fewer than four classified, internal Defense Department e-mail systems….The virus affected NASA and CIA on its two hour race around the world, three times faster than its predecessor Melissa. The virus is estimated to have ultimately affected over forty-five million users in more than twenty countries. The various estimates of the damage caused, ranging from two billion dollars to ten billion, reflect on the inherent difficult of assessing the harm inflicted by cybercrime.[90]

2.1.3 Unrestricted jurisdiction

As noted:

> Unlike real-world 'crime', cybercrime does not require any degree of physical proximity between the victim and the victimizer at the moment the crime is committed. Cybercrime is unbounded crime, borderless crime. It can be committed by someone who is located anywhere in the world against a victim who is in another city, another state, another country. All the perpetrator requires is access to a computer that is linked to the Internet; with this, he can inflict 'harm' upon someone directly, by attacking their computer, say, indirectly, by obtaining information that lets him assume their identity and use it to commit fraud on a grand scale.[91]

---

[89] See, for example, Brenner note 15. See also the discussion of the 'Love Bug' virus at 1.1 above.
[90] See Lev Grossman 'Attack of the love bug' (15 May 2000) available at http://www.time.com/time/magazine/article/0,9171,996899-6,00.html [Accessed 16 January 2007]. See also Goodman note 15.
[91] Susan W Brenner 'Toward criminal law for cyberspace: A new model of law enforcement' (2004) 30 *Rutgers Computer and Technology Law Journal* 1 at 25-26.

In the networked world crime is not confined within boundaries, since a criminal does not have to be physically present in a jurisdiction to commit a cybercrime.[92] A cybercrime can be committed from anywhere and against any 'computer' user in the world; a very attractive characteristic for criminal activity.[93] A criminal is able to commit crimes across international borders with a level of anonymity, and the scene of crime becomes difficult to identify.[94] Tracing and identifying a criminal in the digital world can be almost impossible, as can the apprehending of the criminal, as this may depend on international cooperation.[95] The distribution of the 'Love Bug' virus affecting more than twenty countries demonstrates how easy it can be to commit crimes across borders.[96] As one study noted:

> Effective law enforcement is complicated by the transnational nature of cyberspace. Mechanisms of cooperation across national borders to solve and prosecute crimes are complex and slow. Cybercriminals can defy the conventional realms of sovereign nations, originating an attack from almost any computer in the world, passing it across multiple national boundaries, or designing attacks that appear to be originating from foreign sources. Such techniques drastically increase both the technical and legal complexities of investigating and prosecuting cybercrimes.[97]

2.1.4 Unclear definition

Most countries' laws are inadequate to prosecute cybercrimes; the existing laws cannot be enforced against such crimes.[98] 'In cyberspace archaic laws often make crime and punishment rather distant relatives.'[99] The traditional classification of existing common law crimes does not cater for the prosecution of cybercrime. A typical example is a denial of service attack, which cannot be prosecuted as vandalism, trespass, burglary, theft, arson, or extortion even though it is a malicious activity, damaging or perhaps even destroying the victim's ability to conduct business.[100] Accordingly:

---

[92] See, for example, McConnell International note 1. See also Williams note 4. Further, see Goodman (note 7) at 471.
[93] See Goodman (note 7) at 471. See also Williams note 4.
[94] See generally Williams note 4. See also Robinson note 7.
[95] See generally McConnell International note 1. See also Robinson note 7.
[96] See the discussion of the 'Love Bug' virus at 1.1 and 2.1.2 above.
[97] McConnell International note 1.
[98] See, for example, McConnell International note 1. See also Goodman note 7. Further, see CNN.com note 49.
[99] CNN.com note 49.
[100] See, for example, Goodman note 15. See also Brenner note 15.

> No 'property' is damaged; there is no intrusion into a protected area (with or without the intent to commit an offence therein); nothing is stolen (at least not in the sense that the perpetrator 'takes' property from the victim and thereby enriches himself at the victim's expense); no fire or explosives are used to damage property; and nothing of value is typically extorted in exchange for ceasing the attack.[101]

Cybercrime yields new and different types of activities capable of evading the reach of existing criminal laws.[102] Criminals can easily exploit gaps in their own country's criminal laws to victimise their fellow citizens with impunity.[103] Criminals can also exploit gaps in other country's criminal laws to victimise the citizens of those and other countries.[104] This was one of the lessons of the 'Love Bug' virus. The author of the virus, Onel de Guzman, a computer programming student in the Philippines, when finally arrested could not be prosecuted under the Philippines laws because no laws prohibited the distribution of a computer virus, even one which destroyed valuable information such as computer files or stole passwords.[105]

2.2 Types of cybercrimes

A cybercrime can be committed by using a computer in three main ways:

- As the target of a crime
- As a tool for a crime
- As incidental to a crime

2.2.1 A computer as the target of a crime

This occurs by attacking the confidentiality, integrity and/or availability of data.[106] The criminal attacks a computer system by breaking into the system and bombarding

---

[101] Goodman note 15.
[102] See ibid.
[103] See ibid.
[104] See ibid.
[105] See ibid. See also 2.1.2 above.
[106] See Brenner note 67. 'Confidentiality' is defined as the property that information (data) is not made available to unauthorised individuals, entities or processes, 'integrity' as the property that data has not been changed, destroyed or lost in an unauthorized or accidental manner and 'availability' as the property of a system (or of a specific system resource) to be accessible and usable whenever required by an authorised entity and according to performance specifications appropriate to the system.

it from outside.[107] Examples include hacking (gaining unauthorised access to a computer system) and cracking (gaining unauthorised access to a computer system to commit another crime such as destroying information in that system).[108] Other examples are data theft, theft of intellectual property (such as trade secrets), the 'Love Bug' virus that damaged computers around the world resulting in great financial loss, and the February 2000 Distributed Denial of Service attacks (DDoS) that were launched against Yahoo, CNN and E-Bay.[109] To carry out a DDoS attack, the attacker uses compromised computer systems to flood the target systems with messages that essentially shut it down.[110] The computer is absolutely essential for committing these crimes; before the advent of the computer these crimes never existed and consequently jurisdictions will need to address these "new" crimes.[111]

2.2.2 A computer as a tool for a crime

Like most tools, computers can be used for criminal purposes.[112] A computer as a tool for a crime occurs by simply using computers, computer systems, and related information and communication technology to commit traditional crimes.[113] Using computers merely facilitates committing the crime. Notably, '[b]y introducing new programming instructions, or manipulating computers' legitimate functions for illegal purposes, perpetrators exploit computers for the commission of crimes.'[114] The use of computer technology as a tool to commit a crime does not alter the nature of the offence. This type covers crimes that are prevalent in the physical world, but that are now increasing on the Internet.[115] These are the traditional crimes such as theft, fraud, forgery, stalking, trafficking, distribution, posting and dissemination of child or other

---

[107] See, for example, Goodman (note 7) at 469.
[108] See, for example, Brenner (note 67) 2.
[109] See, for example, Goodman (note 7) at 469. See also Brenner (note 67) 2. Further, see the discussion of the 2000 February DDoS attack and the 'Love Bug' virus at 2.1.2 above.
[110] See, for example, SearchSecurity.com 'Distributed denial of service attack.' Available at *http://searchsecurity.techtarget.com/sDefinition/0,,sid14_gci557336,00.html* [Accessed 22 January 2007].
[111] See, for example, Brenner (note 67) 3.
[112] See, for example, Goodman (note 7) at 467.
[113] See, for example, Brenner (note 67) 3. See also Goodman note 15.
[114] Ferrera note 75 at 302.
[115] See, for example, Robinson note 7.

pornography, intellectual property violations and even murder.[116] These crimes are not substantially 'new' but existing criminal laws may not be adequate to prosecute these crimes; therefore, states will have to adjust their laws.[117]

2.2.3 A computer as incidental to a crime

A computer is not essential for committing a crime in this category.[118] These are traditional crimes that have existed long before computers did, but a computer may still be of significant use in committing the crime.[119] The use of a computer allows for the more efficient commission of a crime, for example, using a computer for illegal book-making, or when a blackmailer uses a computer to generate blackmail letters or e-mails.[120] Some view this category as not representing a 'true' variety of cybercrime because the computer plays a peripheral role and, as a result, adoption of new substantive cybercrime law is hardly required for the apprehension and prosecution of the culprit.[121] Although this may be the case, crimes of this type still pose challenges for law enforcement by increasing the investigative work involved whenever computer technology is used for illegal purposes.[122] Other 'incidental' cybercrimes include paedophiles' child pornography records and drug dealers' financial records on their computers.[123]

2.3 Categories of cybercrimes

In many instances cybercrimes overlap, but basically, they are divided into three major categories:

- Cybercrimes against persons

---

[116] See, for example, Brenner (note 67) 3. See also Ferrera (note 74) 302. Further, see Goodman (note 7) at 469 and Robinson note 7.
[117] See, for example, Brenner (note 67) 3.
[118] See, for example, Ferrera (note 74) 303.
[119] See, for example, ibid. See also Goodman (note 7) at 469.
[120] See, for example, Ferrera (note 74) 303.
[121] See, for example, Brenner (note 67) 2.
[122] See, for example, Brenner (note 67) 2. See also Robinson note 7.
[123] See, for example, Goodman (note 7) at 469. See also Robinson note 7.

- Cybercrimes against property
- Cybecrimes against Government

2.3.1 Cybercrimes against persons

This category deals with cybercrimes committed against persons. Typical examples are:

- Obscene material/pornography
- Cyber-harassment
- Cyber-stalking
- Hate speech

Obscene material/pornography involves the trafficking, distribution, posting, and dissemination of obscene material including pornography, indecent exposure, and child pornography.[124] This type of crime is one of the most serious cybercrimes; its potential effects can hardly be overstated.[125] Paedophiles carry out many activities over the Internet, including viewing images, discussing activities, arranging tourism, and enticing a child to a meeting.[126] The transnational nature of the Internet affords child molesters and pornographers unlimited opportunities to target and recruit new victims. It allows sexual predators to stalk minors discreetly from their homes. Unquestionably, this is the reality: '[a] minor girl in Ahmedabad was lured to a private place through cyberchat by a man, who, along with his friends, attempted to gangrape her. As some passersby heard her cry, she was rescued.'[127] Clearly, this crime is harmful to minors and, if not controlled, it could have extremely damaging effects.

Cyber-harassment is a malicious offence; it involves sending repeated, threatening or harassing messages using cyberspace, and targeting a particular

[124] See, for example, Susan Brenner 'Cybercrimes against persons.' Available at http://www.cybercrimes.net/Persons/persons.html [Accessed 6 April 2006]. See also Duggal note 5.
[125] Duggal note 5.
[126] See Goodman note 15.
[127] Babu note 67.

person.[128] It can be sexual, racial, religious, or another type of harassment,[129] as this infamous California case illustrates:

> An honors graduate from the University of San Diego terrorized five female university students over the Internet for more than a year. The victims received hundreds of violent and threatening e-mails, sometimes receiving four or five messages a day. The graduate student … told police he committed the crimes because he thought the women were laughing at him and causing others to ridicule him. In fact, the victims had never met him.[130]

This crime is closely related to the issue of the violation of privacy of netizens.[131] Privacy is valuable and close to the heart of every citizen, and the law protects people's privacy, but the Internet can allow for this privacy to be violated.[132]

Cyber-stalking is also a malicious offence that involves the crime of stalking by using a computer and the Internet, and the offence is aimed at a specific person.[133] Another notorious California case illustrates this offence:

> [A] 50-year-old former security guard … used the Internet to solicit the rape of a woman who rejected his romantic advances …. [H]e terrorized his 28-year-old victim by impersonating her in various Internet chat rooms and online bulletin boards, where he posted, along with her telephone number and address, messages that she fantasized of being raped. On at least six occasions, sometimes in the middle of the night, men knocked on the woman's door saying they wanted to rape her….[134]

Hate speech is the dissemination of threatening hate-filled messages targeting people merely on account of their race, colour, sex, religion, ethnicity, or sexual orientation.[135] Hate speech is focused more generally, but it is still traumatic for those against whom it is levelled, and it is spreading widely, with the aid of the Internet. For example:

---

[128] See, for example, Babu note 67. See also Brenner note 124. Further, see the U.S. Department of Justice, 'Cyberstalking: a new challenge for law enforcement and industry' (August 1999). Available at http://www.usdoj.gov/criminal/cybercrime/cyberstalking.htm. This crime can be committed through e-mail, use of websites, or chat programs.
[129] See, for example, Babu note 67. See also Duggal note 5.
[130] The U.S. Department of Justice note 128. See also Goodman note 15.
[131] See, for example, Babu note 67. See also Duggal note 5. 'Netizens' are the citizens of the Internet, or people using the Internet.
[132] Almost all Constitutions protect the right to privacy.
[133] See, for example, Brenner note 124. See also Goodman note 15. Cyberstalking broadly refers to engaging in a course of conduct causing a reasonable person to suffer intimidation or serious inconvenience, annoyance or alarm, as well as fearing death or injury to themselves or their family. Further, see Brenner (note 67) 30.
[134] The U.S. Department of Justice note 128. See also Goodman note 15.
[135] See, for example, Ferrera (note 74) 305.

> The e-mail address of a group of Jewish students in Germany was bombarded with more than 17,000 messages from adolf@hitler.com containing a threat to repeat the Holocaust. The murder of six million Jews, the sender threatened, would start Nov. 9 - the anniversary of Kristallnacht, the Nov. 9, 1938 'Night of Broken Glass' when Nazi regime orchestrated attacks on Jews and Jewish businesses across Germany in a harbinger of the Holocaust. Germany's cyber police conceded they were powerless to investigate because the e-mails were sent via a server in the U.S., material that falls outside German laws that make Neo-Nazi propaganda a crime. Germany has repeatedly complained that United States free speech laws have crippled its efforts to stop the spread of Neo-Nazi ideas via the Internet.[136]

2.3.2 Cybercrimes against property

This category involves cybercrimes against all forms of property. These are crimes committed against the confidentiality, integrity and/or availability of data and systems. These crimes include:

- Hacking and cracking
- Denial of service and distributed denial of service
- Virus dissemination
- Sabotage
- Extortion
- Industrial espionage
- Forgery
- Fraud
- Software and other copyright infringement

Hacking and cracking are aimed at accessing a system or data. Hacking refers to unauthorised access to computers, and tampering with precious confidential data and information.[137] Hackers generally enter systems merely for the personal satisfaction of penetrating them, and seldom damage them.

---

[136] Goodman note 15 (citing Arnaud de Borchgrave et al 'Cyber threats and information security: meeting of the 21st century challenge v Center for Strategies and International Studies (2000) at *http://www.csis.org/pubs/2001_cyberthreatsandis.htm*).

[137] See, for example, Duggal note 5.

Cracking involves using various programs and programming abilities with the malicious intent to break into a system.[138] Crackers intend to cause damage when accessing online systems. They may bring computers to a grinding halt, or make copies of sensitive information for unlawful use. Hacking and cracking are not only security-related issues but also constitute an invasion of privacy, since hackers and crackers tamper with precious confidential data without the knowledge and consent of the owner.[139] Unfortunately, no computer is cracking proof.[140] The denial of service attacks experienced by the popular commercial sites like Yahoo, CNN and E-Bay are notable examples of this type of cybercrime.[141]

Denial of service and distributed denial of service result from transmitting too many e-mails, causing the recipients' computers to crash.[142] This is committed by first breaking into the system or network. The February 2000 Distributed Denial of Service attacks launched against Yahoo, CNN, E-Bay and others, causing massive business disruption, are by far the biggest ever.[143] In another incident in 1999, a group of people calling themselves the Electrohippies organised a Distributed Denial of Service attack on the World Trade Organization (WTO).[144] The Electrohippies set up a site, a virtual sit-in, to help tie up the WTO's Web servers. Clicking on the sit-in link made a user's computer request information continually from WTO servers, thus tying up the user's Internet connection.[145] Clearly, '[t]his was essentially the use of hacker's denial-of-service techniques to perform an act of (in their words) civil disobedience in the shape of an electronic sit-in.'[146] Sometimes, these attacks can be automated by using someone's computer unknowingly as the cyber-hippies did.[147]

---

[138] See, for example, Susan Brenner 'Cybercrimes against property.' Available at http://www.cybercrimes.net/Property/property.html [Accessed 6 April 2006]. See also Duggal note 5.
[139] See, for example, Duggal note 5.
[140] See, for example, Babu note 67. See also Duggal note 5. A typical example is the infamous case of Kevin Mitnick, who was arrested and held without trial for approximately $300 million damage caused by copying proprietary software from computers owned by cellular telephone manufacturers and illegally accessing other computer systems. Further, see the U.S. Department of Justice 'Kevin Mitnick sentenced to nearly four years in prison; computer hacker ordered to pay restitution to victim companies whose systems were compromised.' Available at http://www.usdoj/criminal/cybercrime/mitnick.htm. [Accessed 22 January 2007].
[141] See, for example, Robinson note 7.
[142] See, for example, Ferrera note 74.
[143] See, for example, Gelbstein note 72. See also Robinson note 7.
[144] See Gelbstein (note 72) 38.
[145] See ibid.
[146] Gelbstein (note 72) 39.
[147] See ibid 27.

Virus dissemination is the introduction of software damaging to systems or data. This refers to the creation and transmission of harmful computer programs which do irreparable damage to computer systems.[148] This includes any program or code doing harm to a system or data. A computer virus is a specific type of malicious code, which replicates itself and inserts copies of new versions into other programs when it is executed with the infected program.[149] A typical example is the 'Love Bug' virus that affected about 45 million computers and caused tremendous damage.[150] Another example is the Melissa virus. This virus first appeared on the Internet in March 1999, spreading throughout computer systems in the United States and Europe, and causing massive damages to computers worldwide.[151]

Sabotage involves the disconnecting, unauthorised modifying or destruction of a network or system, which can even be done without a physical presence.[152] A hacker with malicious intent can disrupt the operating of crucial items by merely corrupting password files, modifying parameters or injecting malicious code.[153] The most serious sabotage occurs when a person accesses a computer room disguised as a maintenance engineer.[154] If security is weak and the person is unaccompanied and unmonitored, the person can cause massive damage in a very short time in a way that can remain undetected for hours.[155]

Extortion involves the use of force and intimidation to threaten to disrupt information and communication systems to induce the victim to give something of value (usually, money).[156] An example is when a blackmailer plants a digital time or logic bomb and threatens to destroy a system unless the victim pays.[157] Another example is an experience of one company in 2001:

---

[148] See, for example, Brenner note 139. See also Duggal note 5.
[149] See Schjolberg (note 56) at 12.
[150] See 2.1.2 above.
[151] See, for example, Babu note 67. See also Gelbstein (note 72) 38.
[152] See, for example, Gelbstein (note 72) 28.
[153] See ibid. Malicious code is an umbrella term for any computer software designed to make computers perform undesired functions. Two notable forms of malicious code are virus and worms. (Viruses use software in the affected machine to replicate and worms are self-replicating). See also Gelbstein (note 72) 18.
[154] See Gelbstein (note 72) 28.
[155] See Gelbstein (note72) 28-9.
[156] See, for example (and generally), Ferrera (note 74) 305.
[157] See, for example, Goodman note 15. A logic bomb is another form of malicious code commonly used in extortion schemes; it remains undetected until it detonates. See also Gelbstein (note 72) 19.

> Universe did not pay the thief A 19-year old Russian student using the name 'Maxim' stole 300,000 credit card numbers from the computer server of CD Universe. Maxim extorted CD Universe by agreeing to destroy the customer data he had stolen in exchange for $100,000 cash. CD quickly enough for his liking, and Maxim published the credit card and customer data of 25,000 victims online. The event was widely reported in the media and was quite damaging to CD Universe's reputation … Maxim still remains at large.[158]

Extortion schemes may sometimes be unsuccessful, but when conducted subtly they incur a low level of risk and considerable gain for the perpetrator.[159] This crime might not be widely reported as companies have a tendency not to expose their vulnerabilities as they fear the effect of such reporting on their reputations. Nonetheless, this crime is likely to increase as criminals exploit the enormous new opportunities that networked systems offer.[160]

Industrial espionage involves breaking into a system or network and stealing information about product development, commercial strategies, staff salaries, and other confidential matters.[161] This can be achieved leaving little or no evidence of the theft.[162] The practice dates back a long way. Ever since the industrial revolution espionage has been a big issue, especially for businesses in a leadership position in a competitive environment requiring sophisticated research.[163] Industrial espionage is rapidly growing because computer systems and networks are used to document experiments and research.[164] The sponsor of the espionage benefits by deriving knowledge worth millions at a minimal expense and with minimal risk.[165] On the one hand, the Internet stores valuable and sensitive information, but it also exposes the information to a high risk of this kind of crime. A typical example is an industrial spy stealing trade secrets to sell to a business rival.

Forgery refers to the illegal inputting, altering, deleting, or suppressing of computer data resulting in apparently authentic data with the intent that it be considered or acted upon for legal purposes as if it were authentic regardless of

---

[158] Goodman note 15 (quoting Criminal threats to E-Commerce 17 INTERPOL January 2001).
[159] See, for example, Williams note 4.
[160] See ibid.
[161] See, for example, Gelbstein (note 72) 30.
[162] See ibid.
[163] See Gelbstein (note 72) 20.
[164] See ibid.
[165] See, for example, Gelbstein note (72) 20.

whether the data is directly readable and intelligible.[166] Examples include fictitious websites that falsely represent themselves as legitimately established companies, assuming a false identity in e-mails for fraudulent purposes, and posting false information on Internet bulletin boards to manipulate stock market prices.[167]

Fraud is using a computer system by inputting, altering, deleting or suppressing computer data or any interference with a computer or with the functioning of a computer system to cause loss of property to another person, with the fraudulent or dishonest intent to illegally obtain an economic benefit for oneself or for another.[168] Fraud usually involves large amounts of money and no physical violence, and when it is done smoothly, fraud stands a good chance of remaining undetected. It could range from misleading offers for all kinds of property to promises and unfounded financial projections.[169] Cybercriminals commit different types of fraud over computer networks, most commonly, credit card fraud, online auction fraud, mail fraud, and bank fraud.

Software and other copyright infringement refers to the taking or copying of data, whether legally protected by other laws, such as privacy and copyright; and to protecting the illegal copying and distributing of legally or illegally obtained software.[170] This activity is actionable regardless of whether any profits are made or contemplated.[171] Distributing illegal and unauthorised software has been further strengthened by the birth of the personal computer and continues to be practised in many countries. Hardware and peripherals can also be copied. Piracy represents a remarkable loss to copyright owners while the thieves stand a good chance of evading

---

[166] See, for example, the 'Council of Europe Convention on Cybercrime ETS 185 Art 7.' Available at http://conventions.coe.int/Treaty/EN/Treaties/Html/185.htm [Accessed 21 August 2006] (hereinafter, 'Convention'). All further references to the articles of the Convention refer to this Convention. See also the discussion of computer forgery at 2.1.1 (Chap 2 below.)

[167] See, for example, Schjolberg (note 56) at 14.

[168] See the Convention (note 166) Art 8. See also the discussion of computer fraud at 2.1.1 (Chap 2 below.)

[169] See, for example, Schjolberg (note 56) at 15. Cybercriminals have also discovered that it is possible to scam money through Internet dating by assuming a false identity (invented or another's) and playing on a person's feelings by promising all kinds of things and asking for money in the process. For instance, they may ask for money to go visit or money to undergo surgery (to go visit afterwards).

[170] See, for example, Brenner note 138. See also Duggal note 5.

[171] In almost every legal system copyright infringement is a criminal offence.

the law, and although nations have taken initiatives against it, the business continues to flourish.[172]

2.3.3 Cybercrimes against Government

Generally, the perpetrators of cybercrimes against Government have political motivations for their activities; however, determining the intent, identity or motivation with certainty is difficult until long after the commission of the offence. Examples include:

- Cyberterrorism
- Extortion
- Espionage

Cyberterrorism is the politically motivated use of computers as weapons or targets resulting in violence against non-combatant targets, by sub-national groups or clandestine agents to influence an audience or cause a government to change its policies.[173] Cyberterrorism also covers attacks destructive or disruptive enough to instil fear comparable to that resulting from a physical act of terrorism, for example, acts leading to death, injury, extended power outages, airplane crashes, or critical loss of confidence in the economy.[174] For instance, a terrorist might break into an air traffic control system and manipulate it, causing plane crashes or collisions or break into computer systems and disrupt domestic banking, the stock exchange and international financial transactions leading to a major loss of confidence in the economy.[175]

Extortion involves threats and disruptions or shut-downs of essential services.[176] This crime manifests itself when a cracker breaks into government

[172] See, for example, Gelbstein (note 72) 30.
[173] See, for example, Clay Wilson 'Computer attack and cyber terrorism: vulnerabilities and policy issues for Congress CRS Report for Congress' in Pauline C Reich (ed) *Cybercrime and Security* (2005) 5.
[174] See ibid.
[175] See, for example, Goodman note 15.
[176] See Ferrera (note 74) 307.

computer systems and starts making demands, altering, disrupting, or shutting down the systems. For instance:

> [t]he Legion of Doom hacking group gained the ability to alter, disrupt, or shut down local telephone service. In one incident, 40 percent of a patient's records were destroyed at a major medical center. In another incident, a teenager gained access to an airport's traffic control system and left it without telephone or data service. Hackers routinely vandalize government Web sites and deface or otherwise destroy them.[177]

Espionage involves spying on government entities or officials.[178] Criminals use this activity to gather military and other intelligence. In one case, the first to make the international headlines, hackers in West Germany were arrested for breaking into the United States Government and corporate computers and selling United States military secrets to the Soviet KGB.[179] Two fellow hacker spies turned in three of the hackers, while the fourth suspected hacker committed suicide when publicly implicated, but because the information stolen was not top secret the hackers were fined and sentenced to probation.[180]

2.4 Other questionable activities

The above list is not comprehensive. It merely outlines the most common criminal activities classified as cybercrime. Numerous other activities are taking place on the Internet about which the law is not always clear. There are concerns about what activities are actually criminal and in which jurisdiction. These activities include:

- Arms and drug dealing
- Hate speech
- Pornography
- Trading in stolen goods
- Money laundering
- Off shore unregulated gambling

---

[177] Ferrera ibid.
[178] See, for example, Ferrera ibid.
[179] See Gelbstein (note 7) 36. The KGB was the State security police of the Union of Socialist Soviet Republics since 1954.
[180] See Gelbstein ibid.

- Political propaganda
- Disinformation
- Spamming

3. Conclusion

As the Internet becomes the medium through which more and more international trade occurs, the opportunities for other activities are likely to grow; undoubtedly, human ingenuity will continue to create new offences. In fact, '[t]he criminal is always a couple of jumps ahead of the policeman. As when the law plugs any of its numerous loopholes, the motivated criminal will always discover new cracks in the armor.'[181] However, in the final analysis, every jurisdiction reserves the right to make its own laws and if the law says an act is criminal (or not), so it is (or is not). As a result, crimes such as harassment, stalking and hate speech committed on the Internet may not necessarily be criminal depending on the jurisdiction.

[181] Gelbstein (note 72) 1.

CHAPTER TWO: INTERNATIONAL EFFORTS ON CYBERCRIME

Overview

Various international and regional governmental organisations have attempted to create ways to harmonise domestic legislation to improve law enforcement's ability to address cybercrime. Particularly, the Organisation for Economic Co-operation and Development (OECD), the Council of Europe (COE), the United Nations (UN), the European Union (EU) and the Group of Eight (G-8) have played leading and significant roles in creating awareness and cooperation in this regard. This chapter describes efforts that have been made to address cybercrime effectively.

1. The Organisation for Economic Co-operation and Development

The OECD is an international organisation of 30 market democracies working together to address the economic, social and governance issues of a globalising world economy, as well as to exploit its opportunities.[182] The OECD initiated the first comprehensive inquiry into the criminal law problems of computer crime on the international level. The organisation has recommended that basic criminal activities

[182] See 'About OECD.' Available at http://www.oecd.org/about/0,2337,en_2649_201185_1_1_1_1_1,00.html [Accessed 3 August 2006]. The OECD originated in 1948 as the Organisation for European Economic Co-operation (OEEC), to help administer the Marshall plan for the re-construction of Europe after World War II. Later its membership was extended to non-European states, and in 1960 it was reformed into the Organisation for Economic Co-operation and Development. See also the 'Marshall Plan Speech.' Available at http://www.oecd.org/document/10/0,2340,en_201185_1876938_1_1_1_1,00html [Accessed 3 August 2006]. Founding members are Austria, Belgium, Canada, Denmark, France, Germany, Greece, Iceland, Italy, Luxembourg, Netherlands, Norway, Portugal, Spain, Sweden, Switzerland, Turkey, United Kingdom and United States and joined later, with year of admission are Japan:1964, Finland:1969, Australia:1971, New Zealand:1973, Mexico:1994, Czech Republic:1995, Hungary:1996, South Korea:1996, Poland:1996, Slovakia:2000. The Republic of China has an observer status on two OECD committees and the Commission of European Union participates in OECD's work, alongside the European Union Member States. By further cooperating with 70 countries, Non Governmental Organisations and civil society the OECD has attained a global reach. See also the 'OECD Member countries.' Available at http://www.oecd.org/document/1/0,2340,en_2649_201185_1889402_1_1_1_1,00.html [Accessed 3 August 2006].

committed on the Internet be criminalised and has also issued guidelines on the security of information systems (the Recommendation of the Council concerning Guidelines for the Security of Information Systems of 26 November 1992, replaced by the Recommendation of the Council concerning Guidelines for the Security of Information Systems and Networks: Towards a Culture of Security on 25 July 2002).[183]

1.1 The OECD Recommendation

In 1983, the OECD in Paris appointed an expert committee to address computer related crime to harmonise European computer crime legislation.[184] From 1983 to 1985, the OECD surveyed the possibility of the international application and harmonisation of criminal laws addressing cybercrime and abuse.[185] In 1986, the committee issued a report, Computer-related Crime: Analysis of Legal Policy in the OECD Area, which surveyed current laws and proposals for reform and recommended a list of acts that countries must criminalise.[186] The list resulted from a comparative analysis of substantive law worldwide and outlined commonly recognised acts, which could constitute a common basis between the different approaches taken by member states, consisting of:

---

[183] See the 'Recommendation of the Council concerning Guidelines for the Security of Information Systems *1992'* (hereinafter, 'Recommendation'). Available at *http://oecd.org/document/19/0,2340,en_2649_201185_1815059_1_1_1_1,00.html* [Accessed 3 August 2006] The OECD Guidelines for the Security of Information Systems 1992 (hereinafter, 'Guidelines') define 'information systems' as computers, communication facilities, computer and communication networks and data and information that may be stored processed, retrieved, or transmitted by them, including programs, specifications and procedures for their operation, use and maintenance. See also the '*OECD Guidelines for the Security of Information Systems 1992.'* Also available at*http://oecd.org/document/19/0,2340,en_2649_201185_1815059_1_1_1_1,00.html* [Accessed 3 August 2006].The 2002 Guidelines do not attempt to define 'information systems'. Further, see the *'OECD Guidelines for the security of information systems and networks: towards a culture of security* 2002.' Available at *http://www.oecd.org/document/42/0,2340,en_2649_201185_15582250_1_1_1_1,00.html* [Accessed 3 August 2006].

[184] See the International review of criminal policy-United Nations Manual on the prevention and control of computer-related crime at B(9) (hereinafter the 'UN Manual'). Available at *http://www.uncjin.org/Documents/EighthCongress.html* [Accessed 3 August 2006]. Also available at *http://www.uncjin.org/8th.pdf* [Accessed 3 August 2006]

[185] See ibid at II(C)(2) 117.

[186] See ibid at II(C)(2) 118.

- the input, alteration, erasure and/or suppression of computer data and/or computer programs made wilfully with the intent to commit an illegal transfer of funds or of another thing of value;

- the input, alteration, erasure and/or suppression of computer data and/or computer programs made wilfully with the intent to commit a forgery;

- the input, alteration, erasure and/or suppression of computer data and/or computer programs, or other interference with computer systems, made wilfully with the intent to hinder the functioning of a computer and/or of a telecommunication system;

- the infringement of the exclusive right of the owner of a protected computer with the intent to exploit commercially the program and put it on the market; and

- the access to or the interception of a computer and/or telecommunication system, made knowingly and without the authorisation of the person responsible for the system, either by infringement of security measures or for other dishonest or harmful intentions.[187]

1.2 The OECD Guidelines

In 1992, the OECD Council and 24 of its Member states adopted the Recommendation of the Council Concerning Guidelines for the Security of Information Systems [hereinafter, 'Recommendation'], to provide a foundational information security framework for the public and private sectors.[188] The Recommendation contains Guidelines for the Security of Information Systems

[187] Ibid.
[188] See the Recommendation note 183. In 1990, the Information, Computer and Communications Policy (ICCP) created the Group of Experts (governmental delegates, scholars in the field of law, mathematics and computer science, and representatives of the private sector, including computer and communication goods and services providers and users) to prepare the Guidelines for the Security of Information Systems. Upon the final submission of the texts the ICCP approved the texts and their transmission to the Council of OECD.

[hereinafter, 'Guidelines'].[189] This framework involves laws, codes of conduct, technical measures, management and user practices, and public education provisions.[190] The Guidelines focus on implementing minimum standards for the security of information systems and request Member countries to reform their penal systems by criminalising misuse of information systems and developing means for international cooperation.[191]

The security of information systems aims to protect information systems users' interests from harm resulting from failures of availability, confidentiality, and integrity.[192]

One of the recommendations of the Guidelines was to review the Guidelines every five years to foster international co-operation on security of information systems and networks related issues.[193]

In 1997, the OECD Directorate for Science, Technology and Industry reviewed the five-year progress made towards implementing the 1992 Guidelines.[194] The review was conducted by a questionnaire issued to OECD Member countries.[195] Among others, the review revealed that the responding countries had difficulties in developing laws and procedures relating to information security because of 'differences in the various legal systems and how they deal with security matters … such as … computer crimes.'[196] The Members generally agreed that the Guidelines were still adequate and need not be revised.[197]

---

[189] See the Recommendation note 183.
[190] See the Guidelines note 183.
[191] See ibid.
[192] The OECD Guidelines define 'availability', as the characteristic of data, information and information systems being accessible and usable on a timely basis in the required manner, 'confidentiality', the characteristic of data and information being disclosed only to authorised persons, entities and processes at authorised times and in the authorised manner and 'integrity', the characteristic of data and information being accurate and complete and the preservation of accuracy and completeness (the 2002 Guidelines do not attempt to define these terms). See the OECD Guidelines, 1992 and 2002, note 183.
[193] See the OECD Recommendation note 183.
[194] See Goodman note 15. The Recommendation suggested '[reviewing] the Guidelines every five years with a view to improving international co-operation on issues relating to the security of information systems'. See also the Recommendation note 183.
[195] See Goodman note 15.
[196] See ibid (citing the OECD Directorate for Science Technology and Industry-Committee for Information Computer and Communications Policy Review of the 1992 Guidelines for the Security of Information Systems 1997 available at http://www.oecd.org/dsti/sti/it/secur/index.htm).
[197] See ibid.

In 2002, the OECD Council recommended adopting the present OECD Guidelines, because the use of information systems and networks and the entire information technology environment had dramatically changed since 1992 when the first Guidelines were adopted.[198] These continuing changes bring significant advantages which also raise new security issues.[199] Hence, the OECD adopted these Guidelines for a greater awareness and understanding of security issues and the need to develop a 'culture of security'.[200] The Guidelines also focus on implementing minimum standards for the security of systems by:

- Promoting a culture of security for participants to protect information systems and networks.

- Alerting members of the risk of information systems, the measures to avoid the risk and the need to adopt and implement such measures.

- Creating confidence among participants in information systems and networks and in the manner they are provided and used.

- Providing reference in understanding security issues and respecting ethical values when developing and implementing coherent security measures for the security of information systems and networks.

- Promoting co-operation and information sharing among participants in developing and implementing security measures.

- Promoting considering security as important among participants involved in developing or implementing standards.[201]

The Guidelines identify nine principles to consider in protecting information systems and providing for their security.[202] The principles are complementary and

[198] See the OECD Recommendation and the Guidelines, 2002 note 183.
[199] See the Guidelines, 2002 note 183.
[200] See the Recommendation and the Guidelines, 2002 note 183.
[201] See the Guidelines, 2002 note 183.
[202] See ibid.

must be read as a whole.[203] They relate to participants at all levels, including policy and operational levels.[204] The principles are:

- *Awareness*

  Participants should be aware of the need for security of information systems and networks and what they can do to enhance security.

- *Responsibility*

  All participants are responsible for the security of information systems and networks.

- *Response*

  Participants should act in a timely and co-operative manner to prevent, detect and respond to security incidents.

- *Ethics*

  Participants should respect the legitimate interests of others.

- *Democracy*

  The security of information systems and networks should be compatible with the essential values of a democratic society.

- *Risk assessment*

  Participants should conduct risk assessments.

- *Security design and implementation*

  Participants should incorporate security as an essential element of information systems and networks.

- *Security management*

  Participants should adopt a comprehensive approach to security management.

---

[203] See ibid.
[204] See ibid.

- *Reassessment*

  Participants should review and reassess the security of information systems and networks, and make appropriate modifications to security policies, practices, measures and procedures.[205]

The 2002 Recommendation replaces the 1992 Recommendation and the Guidelines will be reviewed again in 2007.[206]

2. The Council of Europe

The COE is an international organisation comprising 46 members, including all the 25 members of the European Union.[207] The COE seeks to promote democracy, and protect human rights and the rule of law throughout Europe.[208] The COE has extensively engaged in the legal issues of computer-related crime.[209]

2.1 The Recommendation No. R. (89) 9

In 1985, the COE appointed an expert committee, the Select Committee of Experts on Computer-Related Crime of the Council of Europe, to discuss cybercrime issues.[210]

---

[205] See ibid.
[206] See the Recommendation, 2002 note 183.
[207] The COE was established in 1949 primarily as a forum to uphold and strengthen human rights, and to promote democracy and the rule of law in Europe. Over the years, the COE has been the negotiating forum for a number of conventions on criminal matters in which the United States has participated. See 'About the Council of Europe.' Available at http://www.coe.int/T/e/Com/about_coe [Accessed 21 August 2006]. Member States are Albania, Andorra, Armenia, Austria, Azerbaijan, Belgium, Bosnia and Herzegovina, Bulgaria, Croatia, Cyprus, Czech Republic, Denmark, Estonia, Finland, France, Georgia, Germany, Greece, Hungary, Iceland, Ireland, Italy, Latvia, Liechtenstein, Lithuania, Luxembourg, Monaco, Netherlands, Norway, Poland, Romania, Russian Federation, San Marino, Serbia, Slovakia, Slovenia, Spain, Sweden, Switzerland, The former Yugoslav Republic of Macedonia, Turkey, Ukraine and United Kingdom. Observer Member States are Canada, Holy See, Japan, Mexico, and United States (status as of 22 August 2006). See also the 'COE's Member States.' Available at http://www.coe.int/T/E/Com/About_Coe/member_states/default.asp [Accessed 22 August 2006].
[208] See About the Council of Europe note 207.
[209] Through Committees and Conventions the COE has discussed cybercrime issues attempting to harmonise law and practice to improve international legal cooperation.
[210] See the UN Manual (note 184) at II(C)(2) 119. From 1985 to 1989 the Select Committee of Experts on Computer-Related Crime of the Council of Europe discussed computer crime's legal problems. The Committee elaborated a report which the European Commission on Crime Problems adopted at its 38th Plenary Session in June 1989. The Select Committee of Experts on Computer-Related Crime of the Council of Europe and the European Commission on Crime Problems' work prepared this

The Committee drafted Recommendation No. (89) 9, which the Council adopted on 13 September 1989.[211] The Recommendation emphasised the importance of a sufficient and quick response to cybercrime, the transborder character of cybercrime requiring harmonising law and practice, and improving international legal cooperation.[212] Furthermore, it emphasised the need for international consensus in criminalising and addressing some cybercrimes.[213] The Recommendation urges Member States to consider the European Committee on Crime Problems' report, particularly the guidelines for national legislatures, when reviewing their legislation or enacting new legislation.[214] The guidelines for national legislatures include a 'minimum list' and 'optional list' of crimes.[215]

2.1.1 The 'minimum list'

The 'minimum list' addresses crimes to be prohibited and prosecuted by international consensus, including:

- *'Computer Fraud'*: The input, alteration, erasure or suppression of computer data or computer programs, or other interference with the course of data processing, that influences the result of data processing thereby causing economic or possessory loss of property of another person with the intent of procuring an unlawful economic gain for himself or for another person;

- *'Computer Forgery'*: The input, alteration, erasure or suppression of computer data or computer programs, or other interference with the course of data processing, in a manner or under such conditions, as prescribed by national law, that it would constitute an offence of forgery if it had been committed with respect to a traditional object of such an offence;

Recommendation, which was adopted at the Ministers' deputies meeting. See also the 'Council of Europe Committee of Ministers Recommendation No. R. (89) 9 on Computer-Related Crime' (hereinafter 'Recommendation 89 (9)'). Available at http://www.coe.int/t/legal_affairs/legal_co-operation/combating_economic_crime/1_standard_settings/Rec_1989_9.pdf [Accessed 21 August 2006]

[211] See Recommendation 89 (9) note 210. See also the UN Manual (note 184) at II(C)(2) 119.

[212] See Recommendation 89 (9) note 210.

[213] See ibid.

[214] See Recommendation 89 (9) note 210. See also the UN Manual (note 184) at II(C)(2) 120.

[215] See the UN Manual (note 184) at II(C)(2) 120.

- *'Damage to Computer Data or Computer Program'*: The erasure, damaging, deterioration or suppression of computer data or computer programs without right;

- *'Computer Sabotage'*: The input, alteration, erasure or suppression of computer data or computer programs, or other interference with computer systems, with the intent to hinder the functioning of a computer or a telecommunication system;

- *'Unauthorised Access'*: The access without right to a computer system or network by infringing security measures;

- *'Unauthorised Interception'*: The interception, made without right and by technical means, of communications to, from and within a computer system or network.

- *'Unauthorised Reproduction of a Protected Computer Program'*: The reproduction, distribution or communication to the public without right of a computer program which is protected by law;

- *'Unauthorised Reproduction of a Topography'*: The reproduction without right of a topography protected by law, of a semi-conductor product, or the commercial exploitation or the importation for that purpose, done without right, of a topography or of a semi-conductor product manufactured by using the topography.[216]

2.1.2 The 'optional list'

The 'optional list' describes prominent offences on which international consensus would be difficult to reach; involving:

- *'Alteration of Computer Data or Computer Programs'*: The alteration of computer data or computer programs without right;

[216] See the UN Manual (note 184) at II(C)(2) 120-1.

- *'Computer Espionage'*: The acquisition by improper means or the disclosure, transfer or use of a trade or commercial secret without right or any legal justification, with the intent either to cause economic loss to the person entitled to the secret or to obtain an unlawful economic advantage for oneself or a third party;

- *'Unauthorised Use of a Computer'*: The use of a computer system or network without right, that either:
  - is made with the acceptance of a significant risk of loss being caused to the person entitled to use the system or harm to the system or its functioning;
  - is made with the intent to cause loss to the person entitled the system or harm to the system or its functioning; or
  - causes loss to the person entitled to use the system or harm to the system or its functioning.

- *'Unauthorised Use of a Protected Computer Program'*: The use without right of a computer program which is protected by law and which has been reproduced without right, with the intent, either to procure an unlawful economic gain for himself or for another person or to cause harm to the holder of the right.[217]

2.2 The Recommendation No. R (95) 13

On 11 September 1995, the COE adopted Recommendation No. R (95) 13 Concerning Problems of Criminal Procedural Law Connected with Information Technology.[218] The Committee of Ministers to Member States presented this Recommendation to guide states and their investigating agencies in the area of information technology by introducing 18 principles organised into seven chapters:

---

[217] See the UN Manual (note 184) at II(C) 120 and 122.
[218] See the 'Council of Europe Committee of Ministers to Member States Recommendation No. R. (95) 13 Concerning Problems of Criminal Procedural Law Connected with Information Technology' (hereinafter 'Recommendation 95 (13)'). Available at http://www.coe.int/t/legal_affairs/legal_co-operation/combating_economic_crime/1_standard_settings/Rec_1995_13.pdf. [Accessed 21 August 2006]. Also available at http://www.privacy.org/pi/intl_orgs/coe/info_tech_1995.html [Accessed 21 August 2006].

- Search and seizure
- Technical surveillance
- Obligations to co-operate with the investigating authorities
- Electronic evidence
- Use of encryption
- Research; statistics and training
- International co-operation[219]

The document focus on these issues when investigating both cybercrime and traditional crimes with evidence found or transmitted in electronic form.[220]

2.3 The Council of Europe's European Committee on Crime Problems

In 1997, the Council of Europe's European Committee on Crime Problems (CDPC) set up a committee of experts (Committee of Experts on Crime in Cyberspace) to deal with cybercrime.[221] The Committee's mandate was to examine laws criminalising cybercrime, to investigate and develop international co-operation regarding information technology, and to reach a common approach.[222] The new committee was also assigned to draft 'a binding legal instrument' addressing these issues.[223]

2.4 The Council of Europe's Committee of Experts on Crime in Cyberspace

In April 1997, the Committee of Experts on Crime in Cyberspace (PC-CY) started its work, preparing a Convention on Cybercrime.[224] Preparing the Convention took four

---

[219] See the Appendix to Recommendation (95) 13 note 218.
[220] See Recommendation (95) 13 note 218.
[221] See the 'Council of Europe Explanatory Report to the Convention on Cybercrime (ETS 185)' (hereinafter, 'Explanatory Report') para 12. Available at http://conventions.coe.int/Treaty/en/Reports/Html/185.htm [Accessed 23 November 2006]. See also Net Dialogue 'COE's Committee of Experts on Crime in Cyber-space.' Available at http://www.netdialogue.org/background/oecccyberspace/index.shtml [Accessed 23 January 2007].
[222] See the Explanatory Report ibid para 11. See also Net Dialogue ibid.
[223] See ibid.
[224] See the 'Council of Europe Committee of Experts on Crime in Cyberspace Final Activity Report' (hereinafter, 'Final Activity Report') (25 May 2001). Available at

years and 28 drafts before the final version, dated 25 May 2001, was submitted to the CDPC at its 50th Plenary Session on 18 to 22 June 2001.[225] The final version contains a Preamble and four Chapters.[226]

Chapter II includes measures to be taken at the national level in Section 1, 'substantive criminal law' and Section 2, 'procedural law'.[227] The Draft Convention contains the Explanatory Memorandum which indicates that Section 1 aims to improve the means of preventing and suppressing computer or computer-related crime by establishing a common minimum standard of relevant offences, beneficial at the national and the international level.[228] In fact, '[c]orrespondence in domestic law may prevent abuses from being shifted to a Party with a previous lower standard. As a consequence, the exchange of useful common experiences in the practical handling of cases may be enhanced, too.'[229] Additionally, harmonisation facilitates international co-operation, especially extradition and mutual legal assistance, for instance, relating to double criminality requirements.[230]

Parties to the Convention would agree to adopt legislation and other measures to criminalise certain computer-related activities under domestic law.[231] Chapter II, sets out these activities in five titles:

- illegal interception of and/or interference with computer data, illegal access to and/or interference with computer systems, and the misuse of devices to commit any of these offences;
- computer-related forgery and fraud;
- child pornography;
- the infringement of copyright and related rights; and

---

http://cryptome.org/cycime-final.html#DRAFT [Accessed 21 August 2006].
[225] See the 'Council of Europe Explanatory Memorandum to the Draft Convention on Cybercrime' (hereinafter, 'Explanatory Memorandum') para 7-15. Available at http://cryptome.org/cycime-final.html#DRAFT%20REPORT [Accessed 6 March 2006].
[226] See the Final Activity Report note 224.
[227] See the Final Activity Report (note 224) at Chap 1-33.
[228] See the Explanatory Memorandum (note 225) para 7-15.
[229] Goodman note 15.
[230] See the Explanatory Memorandum (note 225) para 7-15.
[231] See the Final Activity Report (note 224) at draft.

- provisions governing the imposition of aiding and abetting and corporate liability.[232]

Parties also agree to establish 'effective, proportionate and dissuasive criminal … sanctions' for the commission of the particular offences.[233]

The Council of Europe Parliamentary Assembly approved the Draft Convention on Cybercrime at its April 2001 Plenary Session, and submitted it for approval to the CDPC at its June 2001 50th plenary session.[234] On 8 November 2001, the Committee of Ministers adopted the Convention and its Explanatory Report at its 109th Session and opened it for signature on 23 November 2001in Budapest, Hungary.[235]

2.5 The Council of Europe Convention on Cybercrime

The Council of Europe Convention on Cybercrime is the first international treaty aimed at specifically addressing several categories of cybercrime.[236] This Convention entered into force on 1 July 2004 and at present, 25 States have signed it (not followed by ratifications) and 18 have ratified it, legally committing themselves to be bound by it.[237] This Convention is open for signature by the member States of the Council of

---

[232] See the Explanatory Memorandum (note 225) para 35.
[233] See the Final Activity Report (note 224) at 1 Title 5 Art 13.
[234] The 'Parliamentary Assembly-reactions and conclusions.' Available at *http://www.coe.int/T/E/Com/Files/Themes/Cybercrime/e_assparl.asp* [Accessed 21 August 2006].
[235] See the Convention note 166.
[236] See the Preamble of the Convention note 166.
[237] See the 'Convention on Cybercrime CETS No.: 185.' Available at *http://www.conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=185&CM=12&DF=1/17/2007&CL=ENG* [Accessed 17 January 2007]. At a signing ceremony on 23 November 2001, 26 member States of the Council of Europe and four observer States (that participated in the negotiations) signed the Convention. The 25 States that have signed the Convention are: Austria, Belgium, Czech Republic, Finland, Germany, Greece, Iceland, Ireland, Italy, Latvia, Luxembourg, Malta, Moldova, Poland, Portugal, Serbia, Slovakia, Spain, Sweden, Switzerland, and United Kingdom (member States of the Council of Europe) and Canada, Japan, Montenegro and South Africa (non-member States of the Council of Europe). The 18 ratifying States are: Albania, Armenia, Bosnia and Herzegovina, Bulgaria, Croatia, Cyprus, Denmark, Estonia, France, Hungary, Lithuania, Netherlands, Norway, Romania, Slovenia, the former Yugoslav Republic of Macedonia, Ukraine (member States of the Council of Europe) and United States (non-member state of the Council of Europe), (status as of 17 January 2007). By signing the Convention Parties agree that they are not opposing it, and yet they are not undertaking to be bound by it. For the Convention to be binding Parties have to sign and ratify it, thus accepting the mandate to implement its provisions. This Convention commits Parties to effective and compatible

Europe and the non-member States which have participated in its negotiations and for accession by other non-member States.[238]

The Convention seeks to pursue a 'common criminal policy' to combat cybercrime, especially by adopting appropriate legislation and fostering international co-operation through:

- harmonising domestic legislation;
- adopting legislation facilitating the preserving and sharing of evidence; and
- improving international co-operation to the 'widest extent possible' in investigating cybercrime.[239]

The Convention contains four chapters.[240]

2.5.1 The Chapters of the Convention

The Convention deals particularly with violations of network security and interception, computer-related forgery and fraud, child pornography and infringements of copyright, organised as follows:

- *Use of terms*

  This chapter defines computer data, computer system, service provider and traffic data.[241]

- *Measures to be taken at domestic level*

  This chapter includes measures at the national level and covers three sections:

---

laws and tools to combat cybercrime, and to cooperating to investigate and prosecute these crimes. See also the U.S. Department of State 'United States joins Council of Europe Convention on Cybercrime' (29 September 2006). Available at http://www.state.gov/r/pa/prs/ps/2006/73353.htm [Accessed 23 November 2006].

[238] See the Convention on Cybercrime CETS No.: 185 note 237. See also 'Frequently asked questions and answers about the Council of Europe Convention on Cybercrime' (hereinafter, 'FAQs on the Convention'). Available at http://usdoj.gov/criminal/cybercrime/COEFAQs.htm [Accessed 17 January 2007] See also the Convention (note 166) Art 36.

[239] See the Preamble of the Convention note 166. See also the Explanatory Report (note 221) para 16.

[240] See the Convention note 166. See also the Explanatory Report note 221.

[241] See the Convention (note 166) Art 1.

- Substantive criminal law

  This section defines nine criminal offences grouped in four categories of computer-related crimes: offences against the confidentiality, integrity and availability of computer data and systems (illegal access, illegal interception, data interference, system interference and misuse of devices), computer-related offences (computer-related forgery and fraud), content-related offences (offences related to child pornography) and offences related to infringements of copyright and related rights (copyright and related rights).[242]

- Procedural law

  This section deals with the procedural aspects, and applies to any criminal offence committed through the use of computer systems and to the collection of evidence in electronic form of a criminal offence.[243] The procedures include the expedited preservation of stored computer data and electronic communications (traffic data), production orders, search and seizure of stored computer data, and real-time collection of computer data.[244]

- Jurisdiction

  This section addresses the issue of jurisdiction to determine where the offence was committed and which law must accordingly apply.[245] Parties must enact legislation to establish jurisdiction relating to offences committed on their territories, on registered ships or aircraft or by their nationals abroad.[246]

- *International co-operation*

  This chapter establishes a rapid and effective system for international co-operation and has two sections:

  - General provisions

    The general provisions include principles relating to mutual assistance, and procedures on mutual assistance requests in the absence of international agreements. The Convention permits law enforcement in one country to

[242] See the Convention (note 166) Arts 2-13.
[243] See the Explanatory report (note 221) para 131.
[244] See the Convention (note 166) Arts 14-21.
[245] See the Explanatory Report (note221) paras 232-33.
[246] See the Convention (note 166) Art 22.

collect computer-based evidence for the law enforcement in another country and deems cybercrimes to be extraditable offences.[247]

- Specific provisions

  The special provisions relate to mutual assistance regarding provisional measures, and to mutual assistance for accessing data, and call for establishing a 24-hour seven-days-a-week contact network to facilitate 'immediate assistance' in 'investigations or proceedings concerning criminal offences related to computer systems and data or for the collection of evidence in electronic form of a criminal offence.'[248]

- *Final clauses*

  The last chapter comprises the final clauses which in limited respects are similar to the standard provisions in the Council of Europe treaties. According to Article 40 any State may declare that it avails itself of the possibility of requiring additional elements as provided for in some articles. Likewise, according to Article 42, any State may declare that it avails itself of the reservations as provided for in some articles.[249]

An additional protocol, addressing acts of a racist and xenophobic nature committed through computer systems, supplements the Council of Europe Convention on Cybercrime.[250]

2.6 The Additional Protocol to the Convention on Cybercrime, Concerning the Criminalisation of Acts of a Racist and Xenophobic Nature Committed through Computer Systems

The Additional Protocol to the Convention on Cybercrime defines racist or xenophobic acts committed through computer networks and makes their publication a

[247] See the Convention (note 166) Arts 23-28.
[248] See the Convention (note 166) Arts 29-35.
[249] See the Convention (note 166) Arts 36-48.
[250] See FAQs on the Convention note 238.

criminal offence.[251] This additional protocol was negotiated in the late 2001 and early 2002, and on 7 November 2002 the Committee of Ministers adopted it.[252] This protocol was opened for signature on 28 January 2003 and is open for signature by the States which have signed the Convention on Cybercrime ETS 185.[253] The protocol entered into force on 1 January 2006 and presently 21 States have signed it (not followed by ratifications) and 10 have ratified it.[254]

The protocol is separate from the main Convention; it does not bind a country that signed and ratified the Convention but not the protocol.[255]

3. The United Nations

The UN is an international organisation of 192 members.[256] It seeks to:

- practice tolerance and live together in peace with one another as good neighbours;
- unite [our] strength to maintain international peace and security;

---

[251] See 'Additional Protocol to the Convention on Cybercrime, concerning the criminalisation of acts of a racist and xenophobic nature committed through computer systems CETS 189' (hereinafter, 'Additional Protocol'). Available at *http://conventions.coe.int/Treaty/en/Treaties/Html/189.htm* [Accessed 22 August 2006]. See also FAQs on the Convention note 238.

[252] See the FAQs on the Convention note 238. The initial draft of the Convention contained language, endorsed by several European countries, criminalising racist websites, but this provision was left out when the United States resisted its inclusion for violating its freedom of speech. Consequently, negotiators agreed to address computer-related hate speech in a separate protocol, which the United States could opt not to sign. However, the United States has expressed reservations to becoming a party to this protocol on constitutional protection grounds.

[253] See FAQs Convention note 238. See also the 'Additional Protocol to the Convention on Cybercrime concerning the criminalization of acts of a racist and xenophobic nature committed through computer systems CETS 189' Available at *http://conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=189&CM=12DF=1/17/2007&CL=ENG* [Accessed 17 January 2007].

[254] See the Additional Protocol note 253. Members that signed the protocol are: Austria, Belgium, Croatia, Estonia, Finland, Germany, Greece, Iceland, Latvia, Luxembourg, Malta, Moldova, Netherlands, Poland, Portugal, Romania, Serbia, Sweden and Switzerland (member States of the Council of Europe) and Canada and Montenegro (non-member States of the Council of Europe). The 10 ratifying States are: Albania, Armenia, Bosnia and Herzegovina, Cyprus, Denmark, France, Lithuania, Slovenia, the former Yugoslav Republic of Macedonia and Ukraine (all member States of the Council of Europe), (status as of 17 January 2007).

[255] See FAQs note 238.

[256] See the 'History of the United Nations.' Available at *http://www.un.org/aboutun/unhistory/* [Accessed 22 August 2006]. The UN officially came into being on 24 October 1945 (celebrated globally as UN day). See the 'List of Member States.' Available at *http://www.un.org/Overview/unmember.html* (status as of 22 August 2006).

- ensure, by the acceptance of principles and the institution of methods, that armed force shall not be used, save in the common interest; and

- employ international machinery for the promotion of the economic and social advancement of all peoples.[257]

The UN has long been a leader in addressing global issues and has engaged in multiple efforts relating to cybercrime.[258] Various bodies within the UN have initiated significant research and negotiations to reach a consensus on a number of cyberspace issues, including setting standards on providing security for networks, and establishing a forum on challenging issues, such as spam and information security.[259]

3.1 The UN Crime Congresses

In 1990, the Eighth UN Congress on the Prevention of Crime and the Treatment of Offenders addressed the legal challenges of cybercrime.[260] The Congress produced a resolution calling for Member States to intensify efforts in combating computer crime, by improving computer security and preventive measures, and promoting the development of a comprehensive international framework of guidelines and standards addressing future computer-related crimes.[261] Most particularly, the resolution calls for Member States to intensify efforts in modernising national criminal laws and procedures, including measures to:

- ensure that existing offences and laws concerning investigative powers and admissibility of evidence in judicial proceedings adequately apply and, if necessary, make appropriate changes;

---

[257] The 'Charter of the United Nations -the Preamble.' Available at http://www.un.org/aboutun/charter/index.html [Accessed 22 August 2006].
[258] For instance, the UN Crime Congresses, the General Assembly and the UN Manual have dealt extensively with this issue. See 3.1-3.2 below. See also Schjolberg (note 56) 6-7.
[259] See, for example, Schjolberg (note 56) 6. See also 3.1-3.3 below.
[260] See the 'Eighth United Nations Congress on the Prevention of Crime and the Treatment of Offenders.' Available at http://www.unjin.org/Documents/EighthCongress.html/#congress [22 August 2006].
[261] See ibid.

- in the absence of laws that adequately apply, create offences and investigative and evidentiary procedures, where necessary, to deal with this novel and sophisticated form of criminal activity; and

- provide for the forfeiture or restitution of illegally acquired assets resulting from the commission of computer-related crimes.[262]

In April 2005, the Eleventh United Nations Congress on Crime Prevention and Criminal Justice reaffirmed the fundamental importance of implementing existing instruments.[263] Further, the Congress reaffirmed developing national measures in criminal matters, such as considering the strengthening and augmenting of measures particularly against cybercrime (among others), as well as extradition, mutual legal assistance and confiscating, recovering and returning crime proceeds.[264] Also, the Congress urged the Members to continue co-operating in combating crime and seeking justice.[265]

3.2 The UN General Assembly

In 1990, the Third Committee of the UN General Assembly prepared a resolution inviting governments to be guided by the resolutions adopted at the Eighth UN Congress in formulating appropriate legislation and policy directives.[266] The General Assembly adopted this resolution on 14 December 1990.[267]

The First, Second and Third Committees of the General Assembly have also passed several resolutions dealing with cyberspace issues. Among these the most relevant are:

---

[262] See ibid
[263] See the 'Eleventh United Nations Congress on Crime Prevention and Criminal Justice.' Available at http://www.un.org/events/11thcongress/declaration.htm [Accessed 25 January 2007].
[264] See ibid.
[265] See ibid.
[266] See Ulrick Sieber 'Legal aspects of computer related crime information society COMCRIME' study prepared under contract with the European Union (19 January 1998) 157. Available at http://europa.eu.int/ISPO/legal/en/comcrime/sieber.doc: [Accessed 22 August 2006].
[267] See Sieber ibid 158.

- Resolutions 53/70 of 4 December 1998, 54/49 of 1 December 1999, 55/28 of 20 November 2000, 56/19 of 29 November 2001, 57/53 of 22 November 2002 and 58/32 of 18 December 2003 on Developments in the Field of Information and Telecommunications in the Context of International Security.[268] These resolutions address concerns that information technology could be used for purposes inconsistent with the goals and principles of the UN. Thus, the resolutions call on States to promote the multi-lateral consideration of existing and potential threats in the field, as well as possible measures limiting the emerging threats.[269]

- Resolutions 55/63 of 4 December 2000, and 56/121 of 19 December 2001 on Combating the Criminal Misuse of Information Technology.[270] These resolutions address different ways in which States could combat the criminal misuse of information technologies.[271] The resolutions urge States to enhance coordination and co-operation in combating the criminal misuse of information technologies.[272] Further, the resolutions note other efforts towards combating these crimes and also note measures adopted to combat these crimes, including, inter alia:
  - coordinated law enforcement cooperation in investigating and prosecuting the criminal misuse of information technologies;
  - legal systems protecting the confidentiality, integrity and availability of data and computer systems from unauthorised impairment and ensuring the penalisation of criminal abuse;
  - legal systems permitting the preservation of and quick access to electronic data in investigating particular cases; and

---

[268] See 'Resolutions 53/70, 54/49, 55/28, 57/53 on Developments in the Field of Information Technology and Telecommunications in the Context of International Security.' Available at *http://www.un.org/documents/ga/res/53/ares53-70.htm* *http://www.un.org/documents/ga/res/54/a54r049.pdf* *http://www.amun.org/undocs/a_res_55_28.*pdf and *http://www.itu.int/wsis/docs/background/resolutions/57-53.pdf* [Accessed 22 Augast 2006], respectively. See also Schjolberg (note 56) 6.
[269] See ibid.
[270] See 'Resolutions 55/63 and 56/121 on Combating the Criminal Misuse of Information Technologies.' Available at *http://www.unodc.org/pdf/crime/a_res_55/res5563e.pdf* and *http://www.unodc.org.pdf/crime/a_res_56/121e.pdf* [Accessed 22 August 2006], respectively. See also Schjolberg (note 56) 6.
[271] See ibid.
[272] See ibid.

- training and equipping law enforcement to address the criminal misuse of information technologies.[273]

- Resolution 57/239 of 20 December 2002 on Creation of a Global Culture of Cybersecurity.[274] This resolution deals with changes in cultural perceptions for achieving greater information and network security; stressing the need for cybersecurity measures and urges States to fulfil nine complementary principles domestically, namely:
  - Awareness
  - Responsibility
  - Response
  - Ethics
  - Democracy
  - Risk assessment
  - Security design and implementation
  - Security management
  - Reassessment[275]

- Resolution 58/199 of 23 December 2003 on Creation of a Global Culture of Cybersecurity and the Protection of Critical Information Infrastructures.[276] This resolution also deals with changes in cultural perceptions for achieving greater information and network security.[277] The resolution notes the interdependence of information infrastructures with other sectors of the global infrastructure that are critical for public services, and encourages States to develop protective strategies for critical infrastructures.[278] The Annex to this resolution provides 11 ways in

---

[273] See ibid.
[274] See Resolution 57/239 available at *http://daccessods.un.org/doc/UNDOC/GEN/NO2/555/22/PDF/N0255522.pdf?OpenElement* [Accessed 22 August 2006].
[275] See the Annex to Resolution 57/239 ibid. The specific actions are organised under those headings (and they resemble the OECD principles). See OECD Guidelines, 2002 note 183. See also 1.2 above.
[276] See 'Resolution 58/199.' Available at *http://daccess.ods.un.org/doc/UNDOC/GEN/NO3/506/52/PDF/N0350652.pdf?OpenElement* [Accessed 22 August 2006].
[277] See ibid.
[278] See ibid.

which States can provide greater protection to critical information infrastructures.[279]

3.3 The UN Manual on the Prevention and Control of Computer-Related Crime

In 1994, the UN Manual on the Prevention and Control of Computer-Related Crime was published.[280] The Manual examines the phenomenon of computer crime, substantive criminal law protecting the holder of data and information, substantive criminal law protecting privacy, human rights, procedural law, crime prevention in the computer environment, and the need for developing international co-operation.[281]

4. The European Union

The EU is a supranational organisation of 25 independent states of the European Communities dedicated to enhancing political, economic and social co-operation.[282]

In 1996 and 1997, the European Commission issued several documents on harmful and illegal content online and on the safe use of the Internet.[283] On 24 April 1997, the European Parliament adopted a resolution on the European Commission's communication on illegal and harmful content on the Internet, supporting the Commission's initiatives and stressing the need for international co-operation in

[279] See the Annex to Resolution 58/199 ibid.
[280] See the UN Manual note 184. See also Sieber note 266.
[281] See the UN Manual note 184.
[282] See the 'European Union.' Available at http://userpage.chemie.fu-berlin.de/adressen/eu.html [Accessed 3 February 2007]. The EU was founded on 1 November 1993, formerly known as European Community (EC) or European Economic Community (ECC). Member States are Austria, Belgium, Bulgaria, Cyprus, Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, Netherlands, Poland, Portugal, Romania, Slovakia, Slovenia, Spain, Sweden and United Kingdom (status as of 3 February 2007).
[283] See Sieber (note 266) 167 For example, the Communication on illegal content online and harmful content confirming that Member States' respective laws will apply to those using the Internet, as they do not operate in a vacuum, and the paper identifies a variety of illegal and harmful content, giving policy options for EU action. Again, the Green Paper on Protection of Minors and Human Dignity on Audiovisual and Information Services addresses the dissemination of content offensive to human dignity and protecting minors against exposure to content harmful to their development.

different initiated areas.[284] Further, in April 1998, the European Commission presented the European Council with a report on computer-related crime which it had commissioned.[285]

In June 2000, the Feira Summit of the European Council adopted the European Commission and European Council's Action Plan.[286] Among other things, the Action Plan calls for establishing a co-ordinated and coherent approach to cybercrime by the end of 2002.[287] A Commission report issued subsequently explains that the EU had planned approximating substantive criminal law in the area of computer-related crime since October, 1999.[288] The report notes that the Commission has been observing the Council of Europe's work on the Draft Convention on Cyber-Crime.[289] Also, it explains that the European Union's plan on approximating substantive cybercrime law could go beyond the C.O.E Convention, representing a minimum of international cooperation, could operate sooner and would bring computer crime in line with EU law, introducing EU law enforcement mechanisms.[290] Further, this portion of the report announces that the European Commission plans to propose:

- Combating child pornography online.[291]

- Approximating hacking and denial of service attacks, and standardising definitions for the EU, to ensure that serious cases are punishable by a minimum penalty in all Member States.[292]

- Acting against racism and xenophobia on the Internet.[293]

---

[284] See Seiber (note 266) 169.
[285] See Goodman note 15. Goodman indicates that this report is called the 'Communication from the European Commission to the Council and the European Parliament: Creating a safer information society by improving the security of information infrastructures and combating computer-related crime' 9 (2000) (hereinafter, 'Creating a safer information society'). Available at *http://europa.eu.int/ISPO/eif/InternetPoliciesSite/Crime/CrimeCommEN.html*.
[286] See ibid.
[287] See ibid (quoting Creating a safer information society).
[288] See ibid (quoting Creating a safer information society).
[289] See ibid (quoting Creating a safer information society).
[290] See ibid (quoting Creating a safer information society).
[291] See Jelle van Buuren 'European Commission wants to tackle cybercrime' (10 January 2001). Available at *http://www.heise.de/tp/english/special/enfo/4658/1.html* [Accessed 24 January 2007]. See also Goodman note 15 (citing Creating a safer information society).
[292] See ibid.

- Considering improving effective efforts against the illicit drugs trade on the Internet.[294]

On 19 April 2002, the Commission of the European Communities presented a proposal for a Council Framework Decision on attacks against information systems.[295] The Council of Europe adopted the proposal on 27 February 2003.[296] The Framework Decision incorporates illegal access to information systems, illegal system interference and illegal data interference.[297]

5. The Group of Eight

The G-8 is a multilateral group consisting of eight of the world's major industrial countries meeting annually to discuss major economic, political and security issues.[298] In 1995, the G-8 formed a group (later called the Lyon Group) to address transnational crime.[299] In 1996, this group produced 40 Recommendations to combat transnational organised crime that the G-8 endorsed in June 1996.[300] Thereafter, the G-8 created the Subgroup of High-Tech crime, among the five 'Subgroups' created to address specific crime related issues.[301] This Subgroup began its work by enhancing the G-8's abilities in preventing, investigating and prosecuting computer related

---

[293] See ibid. The Committee drafting the Convention did not include provisions concerning disseminating online racist and xenophobic material, but they were later addressed in the additional protocol. See the Convention note 166 and the Additional Protocol note 251.
[294] See ibid. The Committee drafting the Convention did not address illicit drug trade on the Internet.
[295] See Schjolberg (note 56) 8.
[296] See ibid.
[297] See ibid.
[298] See the 'Meeting of G-8 Justice and Home Affairs Ministers Washington background on G8' (11 May 2004). Available at *http://www.usdoj.gov/criminal/cybercrime/g82004/g8_background.html* [Accessed 5 September 2006]. The Group of Eight countries are the G-7 nations, Canada, France, Germany, Italy, Japan, United Kingdom and United States (which account for about 2/3 of the world's economic output) and Russia (joined 1997, although a member it does not participate in financial and economic discussions,; it has the smallest economy of the eight nations). The EU is not a member but its representatives attend meetings as 'observers'. The G-8 has met since 1975. See also USINFO.STATE.GOV 'Group of 8 (G8).' Available at *http://usinfo.state.gov/ei/economic_issues/group_of_8.html* [Accessed 5 September 2006].
[299] See the Meeting of G-8 Justice and Home Affairs Ministers Washington background on G8 note 298.
[300] See ibid. Among others, the Lyon Group recommends members to review their laws to ensure criminalising abuses of modern technology.
[301] See ibid.

crimes.[302] In 1997, the G-8 meeting in Washington D.C. adopted ten Principles and an Action Plan to combat high-tech crimes, and further pledged to review their laws in order to criminalise and prosecute these crimes, (among other things).[303]

5.1 The G-8 Principles

The principles adopted to ensure that no country provides 'safe havens' are that:

- There must be no safe havens for those who abuse information technologies.
- Investigation and prosecution of international high-tech crimes must be coordinated among all concerned States, regardless of where [the] harm has occurred.
- Law enforcement personnel must be trained and equipped to address high-tech crimes.
- Legal systems must protect the confidentiality, integrity, and availability of data and systems from unauthorized impairment and ensure that serious abuse is penalised**.**
- Legal systems should permit the preservation of and quick access to electronic data, which are often critical to the successful investigation of crime.
- Mutual assistance regimes must ensure the timely gathering and exchange of evidence in cases involving international high-tech crime.
- Transborder electronic access by law enforcement to publicly available (open source) information does not require authorisation from the State where the data resides.

---

[302] See ibid.
[303] See the 'Meeting of the Justice Ministers of the Eight' (9-10 December 1997). Available at *http://www.usdoj.gov/criminal/cybercrime/g82004/97/communique.pdf* [Accessed 5 September 2006].

- Forensic standards for retrieving and authenticating electronic data for use in criminal investigations and prosecutions must be developed and employed.

- To the extent practicable, information and telecommunications systems should be designed to help prevent and detect network abuse, and should also facilitate the tracing of criminals and the collection of evidence.

- Work in this area should be coordinated with the work of other relevant international fora to ensure against [the] duplication of efforts.[304]

In May 2000, the G-8 held a cybercrime conference discussing how to jointly tackle Internet crime.[305] Bringing together about 300 judges, police personnel, diplomats and business leaders from the G-8 countries, the conference drafted an agenda for a follow-up summit to be held in July.[306] At the July 2000 summit, the G-8 issued a communiqué, declaring that it would 'take a concerted approach to high-tech crime, such as cybercrime, which could seriously threaten security and confidence in the global information society.'[307] The communiqué noted that the G-8's approach to these matters was outlined in paragraph eight of the Okinawa Charter on Global Information Society:

> International efforts to develop a global information society must be accompanied by co-ordinated action to foster a crime-free and secure cyberspace. We must ensure that effective measures, as set out in the OECD Guidelines for Security of Information Systems, are put in place to fight cyber-crime. G-8 co-operation within the framework of the Lyon Group on Transnational Organised Crime will be enhanced. We will further promote dialogue with industry building on the success of the recent G8 Paris Conference…. Urgent security issues such as hacking and viruses also require effective policy responses. We will continue to engage industry and other stakeholders to protect critical information infrastructures.[308]

Additionally, the G-8 pledged establishing a 'Digital Opportunity Taskforce' which would explore integrating the G-8 members' efforts into 'a broader

---

[304] See ibid.
[305] See Goodman note 15 (quoting 'the Group of eight meets to discuss international cooperation on cybercrime' Adlaw by request (May 2000) available at http://adlawbyrequet.com/international/G8Cybercrime.shtm).
[306] See Goodman note 15.
[307] The 'G8 Communiqué Okinawa 2000' (23 July 2000). Available at http://www.g8.utoronto.ca/summit/2000okinawa/finalcom.htm [Accessed 5 September 2006].
[308] The 'Okinawa Charter on Global Information Society 8.' Available at http://www.g8.utoronto.ca/summit/2000okinawa/gis.htm [Accessed 5 September 2006].

international approach'.[309] The Taskforce held meetings during late 2000 and early 2001 and submitted a report containing their Proposed Plan of Action to the personal representatives of the G-8 leaders in May 2001.[310] However, the report did not address cybercrime, but focused instead on the need to overcome the 'digital divide.'[311]

In May 2003, the G-8 adopted Principles for Protecting Critical Information Infrastructures, encouraging counties to consider them in developing a strategy for reducing risks to critical information infrastructures:

- Countries should have emergency warning networks regarding cyber vulnerabilities, threats, and incidents.

- Countries should raise awareness to facilitate stakeholders' understanding of the nature and extent of their critical information infrastructures, and the role each must play in protecting them.

- Countries should examine their infrastructures and identify interdependencies among them, thereby enhancing protection of such infrastructures.

- Countries should promote partnerships among stakeholders, both public and private, to share and analyze critical infrastructure information in order to prevent, investigate, and respond to damage to or attacks on such infrastructures.

- Countries should create and maintain crisis communication networks and test them to ensure that they will remain secure and stable in emergency situations.

- Countries should ensure that data availability policies take into account the need to protect critical information infrastructures.

- Countries should facilitate tracing attacks on critical information infrastructures and, where appropriate, the disclosure of tracing information to other countries.

---

[309] See ibid.
[310] See Goodman note 15.
[311] See ibid.

- Countries should conduct training and exercises to enhance their response capabilities and to test continuity and contingency plans in the event of an information infrastructure attack and should encourage stakeholders to engage in similar activities.

- Countries should ensure that they have adequate substantive and procedural laws, such as those outlined in the Council of Europe Cybercrime Convention of 23 November 2001, and trained personnel to enable them to investigate and prosecute attacks on critical information infrastructures, and to coordinate such investigations with other countries as appropriate.

- Countries should engage in international cooperation, when appropriate, to secure critical information infrastructures, including by developing and coordinating emergency warning systems, sharing and analysing information regarding vulnerabilities, threats, and incidents, and coordinating investigations of attacks on such infrastructures in accordance with domestic laws.

- Countries should promote national and international research and development and encourage the application of security technologies that are certified according to international standards.[312]

On 11 May 2004, the Justice and Home Affairs Ministers and the European Commissioner met in Washington D.C., to discuss combating cybercrime and enhancing cybercrime investigations, among other things.[313] Closing this meeting the Ministers issued a joint communiqué stating that with the Council of Europe Convention on Cybercrime coming into force, the States must encourage the broad adoption of the Convention's legal standards.[314] In June 2005, the Justice and Home

[312] See the 'G8 Principles for Protecting Critical Information Infrastructures.' Available at *http://www.usdoj.gov/criminal/cybercrime/g82004/G8_CIIP_principles.pdf* [Accessed 10 October 2006].
[313] See the 'Meeting of G8 Justice and Home Affairs Ministers.' (10-11 May 2004). Available at *http://www.usdoj.gov/criminal/cybercrime/g82004/index.html* [Accessed 5 September 2006]. Other primary topics were preventing terrorism and serious criminal acts, border and transportation security and fighting foreign official corruption and recovering stolen national assets.
[314] See the 'G8 Meeting Justice and Home Affairs Ministers.' Available at *http://www.privacyinternational.org/article.shtml?cmd[347]=x-347-137754* [Accessed 26 January 2007].

Affairs Ministers meeting in Sheffield discussed international co-operation in combating high-tech crime, among other things.[315]

6. Conclusion

Except for the Convention on Cybercrime, the above initiatives are not binding on countries; they merely provide guidance for an effective framework capable of addressing cybercrime. Therefore, Lesotho can intelligently borrow from these initiatives to enact a comprehensive legal structure to combat cybercrime.

[315] See Privacy International the 'G8 meeting of the Justice Ministers begins–declaring laundry list.' Available at *http://www.privacyinternational.org/article.shtml?cmd[347]=x347-243494&als[theme]=cc%20Home%20Page* [Accessed 23 January 2007].

CHAPTER THREE: NATIONAL LEGISLATIONS ON CYBERCRIME

Overview

Many nations have adopted legislation dealing with all or at least some aspects of cybercrime. These are mainly developed countries; relatively few developing countries have done so. A study published in December 2000 found that of the 52 countries surveyed to determine the state of cybercrime security laws, 33 had not updated their laws to address any type of cybercrime. Nine countries had partially updated theirs, addressing five or fewer types of cybercrime, while the remaining ten had updated their laws on six or more types of cybercrime.[316] McConnell International illustrates the laws that have been updated in each of the 19 countries with fully, substantially, or partially updated laws in place thus:

[316] McConnell International note 1.
No Updated Laws (33): Albania, Bulgaria, Burundi, Cuba, Dominican Republic, Egypt, Ethiopia, Fiji, France, Gambia, Hungary, Iceland, Iran, Italy, Jordan, Kazakhstan, Latvia, Lebanon, Lesotho, Malta, Moldova, Morocco, New Zealand, Nicaragua, Norway, Romania, South Africa, Sudan, Vietnam, Yugoslavia, Zambia, Zimbabwe.
Partially Updated Laws (9): Brazil, Chile, China, Czech Republic, Denmark, Malaysia, Poland, Spain, United Kingdom.
Substantially or Fully Updated Laws (10): Australia, Canada, Estonia, India, Japan, Mauritius, Peru, Philippines, Turkey, and United States.
McConnell International divides cybercrime into four categories, with ten types of the crime, as follows:

- Data Crimes: data interception, data modification and data theft.
- Network Crimes: network interference and network sabotage.
- Access Crimes: unauthorized access and virus dissemination.
- Related Crimes: aiding and abetting cyber crimes, computer-related forgery and computer-related fraud.

Figure 1: Countries with Updated Laws

Countries with Updated Laws										
	Data Crimes			NetworkCrimes		Access Crimes		Related Crimes		
Country	Data Interception	Data Modification	Data Theft	Network Interference	Network Sabotage	Unauthorized Access	Virus Dissemination	Aiding and Abetting Cyber Crimes	Computer-Related Forgery	Computer-Related Fraud
Australia	✓	✓	✓	✓		✓			✓	✓
Brazil		✓			✓	✓		✓		
Canada	✓	✓	✓	✓	✓	✓	✓			✓
Chile	✓	✓	✓	✓	✓					
China		✓		✓			✓			
Czech Republic		✓	✓		✓	✓				✓
Denmark		✓		✓						✓
Estonia		✓	✓	✓	✓	✓	✓	✓		✓
India		✓	✓	✓	✓	✓	✓	✓		✓
Japan	✓	✓	✓	✓	✓	✓		✓	✓	✓
Malaysia		✓				✓		✓		✓
Mauritius	✓	✓		✓	✓	✓	✓	✓	✓	
Peru	✓	✓	✓	✓	✓	✓				✓
Philippines	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Poland		✓	✓	✓				✓		
Spain	✓	✓	✓					✓		✓
Turkey		✓	✓	✓	✓		✓	✓	✓	✓
United Kingdom		✓		✓	✓	✓		✓		
United States	✓	✓	✓	✓	✓	✓	✓	✓		✓

McConnell International also provides a key for Figure 1:

Key for Figure 1

Data Interception: Interception of data in transmission.
Data Modification: Alteration, destruction, or erasing of data.
Data Theft: Taking or coping data, regardless of whether it is protected by other laws, e.g., copyright, privacy, etc.
Network Interference: Impeding or preventing access for others. The most common example of this action is instigating a distributed denial of service (DDOS) attack, flooding Web sites or Internet Service Providers. DDOS attacks are often launched from numerous computers that have been hacked to obey commands of the perpetrator.
Network Sabotage: Modification or destruction of a network or system.
Unauthorized Access: Hacking or cracking to gain access to a system or data.
Virus Dissemination: Introduction of software damaging to systems or data.
Aiding and Abetting: Enabling the commission of a cybercrime.
Computer-Related Forgery: Alteration of data with intent to represent as authentic.
Computer-Related Fraud: Alteration of data with intent to derive economic benefit from its misrepresentation.
[317]

[317] McConnell International ibid.

This chapter reflects some countries' progress in reforming their legal systems to specifically incorporate cybercrime. It does not attempt to analyse the extent to which those countries' penal legislation can be applied to prosecute those using computer technology to commit conventional offences such as theft, fraud and forgery. This chapter discusses the relevant legislation in the United Kingdom, the United States and South Africa.[318]

1. The United Kingdom

The United Kingdom's centrepiece cybercrime legislation is set out in the Computer Misuse Act of 1990 (c. 18). The Act came into effect in 1990 following the leading English case involving computers, *R v Gold* [1987] 3 WLR 803. Further, the United Kingdom regulates other cybercrimes through the Protection of Children Act of 1978 (c 37) (as amended by the Criminal Justice and Public Order Act of 1994 (c. 33) and the Sexual Offences Act of 2003 (c. 42)) and the Copyright, Designs and Patents Act of 1988 (c. 48).

1.1 *R v Gold*

In this case, the defendants, Robert Schifreen and Stephen Gold, using a conventional home computer and a modem in late 1984 and early 1985, gained unauthorised access to British Telecom's (BT) Prestel interactive viewdata service. According to Higney, '[i]t had all started so innocently, with Robert fooling around on his computer back in 1985. 'I never set out to be a hacker, I was testing a home micro computer at a time looking into systems when I stumbled upon a correct password that wasn't mine,' he [Robert] explains.'[319] The BT Prestel system recognised the defendants as legitimate

[318] The United Kingdom being partially updated, the United States substantially updated and South Africa (partially updated) since it is one of the first African countries to adopt this legislation; it could possibly serve as a model for Lesotho. See McConnell International ibid. South Africa enacted cybercrime legislation in 2002. See also the Electronic Communications and Transactions Act 25 of 2002 (hereinafter 'ECTA'). Available at *http://www.info.gov.za/gazette/acts/2002/a25-02.pdf* [Accessed 17 October 2006].

[319] Francis Higney 'Interview with Robert Schifreen' (11-13 October 2006). Available at *http://www.legalitforum.com/ipi/legalitforumv2/index.jsp?pageid=litf_bulletin_015* [Accessed 17 October 2006].

users and suddenly allowed them into its computer systems, and the two obtained passwords of various people in the Prestel organisation. The defendants were arrested and prosecuted under the Forgery and Counterfeiting Act of 1981, for defrauding BT by creating a 'false instrument', as they entered the customer's authorisation code to access the system.[320] The Southwark Crown Court found the defendants guilty.

The defendants appealed to the High Court on the grounds of lack of evidence showing the two had attempted to derive material benefit from their exploits, and on the grounds that the Forgery Act had been misapplied to their conduct. Lord Justice Jane acquitted the defendants, but the prosecution then appealed against that decision to the House of Lords. However, the Law Lords affirmed the acquittal, deciding that the appellants 'had committed no offence under any legislation at that time.' Lord Brandon ruled:

> We have accordingly come to the conclusion that the language of the Act was not intended to apply to the situation which was shown to exist in this case. The submissions at the close of the prosecution case should have succeeded. It is a conclusion which we reach without regret. The Procrustean attempt to force facts into the language of an Act not designed to fit them produced grave difficulties for both judge and jury which we would not wish to see repeated. The appellants' conduct amounted in essence, as already stated, to dishonestly gaining access to the relevant Prestel data bank by a trick. That is not a criminal offence. If it is thought desirable to make it so, that is a matter for the legislature rather than the courts.[321]

As the law then stood, hacking was not a criminal offence. Thus this case set in motion the reform of the criminal law to avoid having to bend traditional interpretations to fit cybercrime.[322]

1.2 The Computer Misuse Act

The Act creates three criminal offences:

- Unauthorised access to computer material

---

[320] The defendants were charged under the Forgery Act since United Kingdom did not have any laws against hacking at the time, and the police also had no idea if the defendants had committed a crime. See Higney ibid.
[321] [1988] AC 1063, at 1069.
[322] Chris Reed and John Angel *Computer law* 4ed (2000) 281-2.

- Unauthorised access to a computer system with intent to commit or facilitate the commission of a further offence

- Unauthorised modification of computer material

1.2.1 Unauthorised access to computer material

This section prohibits intentionally causing a computer to perform any function to access a computing system without any authority.[323] Consequently, hacking becomes criminal regardless of where the hacker operates; locally or long distance over the remote area networks. As such, employees or students with limited authorisation to use their computers but knowingly exceed that authority commit an offence. For instance, without proper authority, the act criminalises:

- using another's identifier (ID) and password to access a computer, using data or running a program;

- altering, deleting, coping or moving a program or data, or merely outputting a program or data to a screen or printer;

- laying a trap to obtain a password; or

- impersonating another person using e-mail, online chat, web, or other services.[324]

The offence is committed when unauthorised access is achieved, and it is punishable on summary conviction by a fine not exceeding 2,000 Pounds, or six months' imprisonment, or both.[325]

---

[323] See the Computer Misuse Act of 1990 (c. 18) s 1. Available at *http://www.hmso.gov.uk/acts/acts1990/Ukpga_19900018_en_1.htm* [Accessed 17 November 2006]. The intent to commit this offence need not be directed at any specific computing system. The Act does not attempt to define 'computer', though it does define 'access.'

[324] The 'University of Liverpool 'The Computer Misuse Act 1990.' Available at *http://www.liv.ac.uk/Regulations/Commisus.html.* [Accessed 17 November 2006].

[325] Access is achieved by merely inducing 'a computer to perform any function' with intent to secure access, without proper authority. See also the Computer Misuse Act s 1(3).

1.2.2 Unauthorised access to a computer system with intent to commit or facilitate the commission of a further offence

This section proscribes gaining unauthorised access with the specific intention to commit or facilitate committing a further offence.[326] For example, a person who illegally accesses a computer using another person's ID to copy legally protected material commits an offence. In *R v Farquharson*,[327] the defendant was prosecuted for obtaining mobile telephone numbers and codes for producing cloned telephones. Actually, Farquharson's co-defendant Ms. Pearce, an employee of the mobile telephone company, had accessed the computing system that contained the information. Pearce was also charged with the s.1 offence.[328] The court found that Farquharson had gained 'unauthorised access' merely by asking Pearce to obtain the information, despite never touching the computer himself.

The offence is committed as soon as the perpetrator obtains specific access for criminal purposes. Upon conviction, a person is liable to imprisonment for up to five years, or a fine, or both.[329]

1.2.3 Unauthorised modification of computer material

This offence criminalises the unauthorised modifying of computer material.[330] This entails deliberately deleting or corrupting programs or data. It also covers introducing viruses, worms and others, which result in modifying or destroying data. Typically, criminal modifications occur by:

- using a trojan horse to obtain identity data or to acquire any data from an unauthorised source;[331]

---

[326] See the Computer Misuse Act s 2.
[327] Croydon Magistrates' Court, 9 December 1993.
[328] See 1.1.1 above.
[329] See the Computer Misuse Act s 2(5).
[330] See the Computer Misuse Act s 3.
[331] A Trojan horse is software which performs legitimate functions but which includes within it malicious code. See Gelbstein (note 72) 19.

- modifying the operating system files or some aspect of the computer's functions to interfere with its operation or to prevent access to any data, including the destruction of files; or

- deliberately generating code to cause a complete system malfunction.

This offence specifically targets those writing and circulating a computer virus or worm, whether operating locally or across networks.[332] Conviction is punishable by imprisonment not exceeding five years, or a fine, or both.[333]

1.3 The Protection of Children Act

This Act regulates child pornography by criminalising taking, permitting to be taken or making, distributing or showing, possessing, publishing or causing to be published any indecent photograph or indecent pseudo-photograph of a child, including by electronic and other means capable of converting into a photograph.[334] The punishment for this offence is imprisonment for a period not exceeding ten years, or a fine, or both.[335]

1.4 The Copyright, Designs and Patents Act

This law criminalises copyright infringement for unlawfully making for selling or hiring, selling, hiring, importing, possessing, offering for selling or hiring, publicly

---

[332] See the University of Liverpool note 324.
[333] See the Computer Misuse Act s 3(7).
[334] See the Protection of Children Act of 1978 (c. 37) s 1 as amended by the Criminal Justice and Public Order Act of 1994 (c. 33) and the Sexual Offences Act of 2003 (42). Available at *http://www.geocities.com.pca_1978/reference/pca_1978amSOA.html* [Accessed 9 January 2007]. The term 'pseudo-photograph' refers to an image, whether made by computer-graphics or otherwise, which can be resolved into an image appearing to be a photograph. The Act stipulates that if the image the pseudo conveys is difficult to classify as either an adult or a child, the prevailing view is that the person shown is a child, to be dealt with as such. This also covers computer-generated and manipulated images. See also ss 7(4)(b), 7(7), 7 (8) and 7(9)(b).
[335] See the Protection of Children Act s 6.

exhibiting, distributing or copying copyright.[336] Under this law copyright also includes a computer program.[337] Criminal liability attaches when:

- infringing a copyright;
- acting without the licence of the copyright owner; and
- committed for commercial purposes.[338]

Conviction is punishable by imprisonment for not more than two years, or a fine, or both.[339]

1.5 Concerns

Since coming into effect the Computer Misuse Act has been successfully applied against the various offences that it was targeting.[340] However, concerns do exist over its wording and its adequacy in fully protecting both systems and data (and yet not restricting the growth of the domestic information technology industry). Concerns include:

- The Act does not define 'computer' potentially incorporating household appliances and cars using computer technology.[341] Nonetheless, the Law Commission recognised that attempting to define 'computer' would be 'so complex, in an endeavour to be all-embracing, that they are likely to produce extensive argument.'[342] Other jurisdictions, such as France and Germany, also adopt this approach while the United States takes exception to this and defines 'computer'.[343]

---

[336] See the Copyright, Designs and Patents Act of 1988 (c. 48) s 107. Available at http://www.opsi.gov.uk/acts/acts1988/Ukpga_19880048_en_21.htm [Accessed 9 January 2007].
[337] See the Copyright, Designs and Patents Act s 3(b).
[338] The Copyright, Designs and Patents Act s 107.
[339] The Copyright, Designs and Patents Act s 107(4).
[340] See Reed (note 322) 290.
[341] See ibid 282.
[342] See ibid.
[343] See ibid 282-3.

- Section 1's is broadly formulated and requires intent to secure access by causing 'a computer to perform any function.' This generally means that by merely interacting with a computer without authorisation, even without specifically and actually accessing any program or data, a person commits an offence.[344] This outlaws all versions of hacking that are designed to crack the security in operating systems, despite the fact that no harm is intended or regardless of the motive. Even mere curiosity or responding to a security system seen as a challenge amounts to a criminal offence.[345] Robert Schifreen mourns the loss of the 'gentleman hacker'–'the hobbyist' without malice, and further notes that illegal hackers seeking to damage people and organisations have replaced the 'social hackers.'[346] Additionally, Schifreen observes that '[t]here are very good hackers out there, Kevin Mitnick, for example, but it is a great waste of their talent. Other people that call themselves hackers simply download programmes or are social engineers. They are not true hackers.'[347] Evidently, however, Schifreen neglected to reflect on hacking as an invasion of privacy and the sense of insecurity felt by the victims.

- The Act needs to be revised as it does not take account of the Internet and does not incorporate offences such as data interception or denial of service (DoS) attacks. The Act does not clearly indicate whether DoS attacks are an offence, creating uncertainty about this grey area and therefore requiring clarity.

---

[344] The only precondition is that the hacker must be aware that the attempted access is unauthorised.
[345] The Gold case is a typical example.
[346] See Higney note 319. See also the discussion of *R v Gold* at 1.1 above.
[347] Higney note 319. Today Robert spends his time hacking in a different style. He is a web editor and writer and often speaks on security issues at conferences, sometimes even sharing a platform with his former arresting officer. He is also a university computer technician. Gold is an independent computer security consultant.
In 1995, Mitnick, a serial cyber-trespasser, was captured by the federal agents for illegally accessing, stealing, copying and misappropriating proprietary computer software. He was kept in prison awaiting trial for four years and became a cause celebre in the hacking underground. In 1999, after pleading guilty on seven counts he was sentenced to little more time to make up for the time he had served while awaiting trial. See, for example, U.S. Department of Justice 'Kevin Mitnick sentenced to nearly four years in prison; computer hacker ordered to pay restitution to victim companies whose systems were compromised' (9 August 1999). Available at *http://www.usdoj.gov.criminal/cybercrime/mitnick.htm* [Accessed 17 January 2007]. See also, John Christensen 'The trials of K Mitnick' CNN (18 March 1999). Available at *http://www.cnn.com/SPECIALS/1999/mitnick.background/* [Accessed 17 January 2007].

The United Kingdom recently amended the Computer Misuse Act with the Police and Justice Act of 2006 (c. 48). The Act was promulgated on 8 November 2006.

1.6 The Police and Justice Act

The Police and Justice Act introduces the following amendments:

- Increased penalty ect for offence of unauthorised access to computer material
- Unauthorised acts with intent to impair operation of computer, etc
- Making, supplying or obtaining articles for use in computer misuse offences
- Transitional and saving provision

1.6.1 Increased penalty ect for offence of unauthorised access to computer material

This section increases the term of imprisonment for hacking into computers from five years to ten years.[348]

1.6.2 Unauthorised acts with intent to impair operation of computer, etc

This section intends to make DoS attacks illegal.[349] As the old law did not clearly indicate whether DoS attacks were an offence, this new section clarifies this issue and specifically indicates that they are an offence. The need for amending this law became apparent when a court threw out the case of a teenager charged for breaching anti-hacking laws by sending five million emails to his former employer. Certainly, the old law had some flaws, '…judges at the Royal Courts of Justice sent the case back to the Magistrates Court, saying Judge Grant was not right to state that there was no case to

[348] See the Police and Justice Act of 2006 (c. 48) s 35. Available at *http://www.opsi.gov.uk/acts/acts2006/20060048.htm* [Accessed 17 November 2006].
[349] See the Police and Justice Act s 36.

answer.'[350] Admittedly, the old law was enacted 16 years ago before cybercrime became a significant problem.

This section replaces section 3 of the Computer Misuse Act.[351]

1.6.3 Making, supplying or obtaining articles for use in computer misuse offences

This section outlaws developing, owning and distributing 'hacker tools' for criminal use.[352] This also covers distributing these tools believing that they are 'likely to be used' criminally.[353] Although this section allows security personnel to have methods of testing the security of systems (as it does not outlaw developing, owning and distributing the tools for legitimate use) it fails to recognise 'dual-use' software that could be used both legitimately and criminally.[354] This is of concern as those distributing these tools (and believing that they are likely to be used criminally) are criminally liable. Despite perhaps being badly drafted, the section objectively seeks to hinder the growing trend in producing and distributing tools more commonly intended to support cybercrimes, and not the legitimate tools.

The majority views this section as 'a bad piece of legislation' that must be removed. Thus for example, some write, '[a]s far as I can see, this looks a complete dog's breakfast of a clause as it fails to consider that many so-called "hacker tools" have perfectly legitimate uses.'[355] Additionally, others stress that:

> With Blears' amendment we've actually gone from a position where a sizeable proportion of a[n] good system administrator's 'toolkit' could be illegal under this new law to one where it almost certainly will be illegal …. Substandard doesn't come close to describing the Committee's handling of this matter.[356]

---

[350] David Meyer 'Email bomber faces retrial' ZDNET UK 11 (May 2006). Available at *http://news.zdnet.co.uk/security/0,1000000189,39268334,00.htm* [Accessed 17 November 2006].
[351] See the Police and Justice Act s 36.
[352] See the Police and Justice Act s 37.
[353] See the Police and Justice Act s 37(2).
[354] This will criminalise both the police and information technology professionals developing and using programs that will later be used for hacking.
[355] Dave Lambert 'Clause 35 is a dog's breakfast.' Available at *http://talkpolitics.users20.donhost.co.uk/index.php?title=another_fine_mess* [Accessed 17 January 2007]. Lambert runs the talk politics blog.
[356] Unity ''Hacker tools' law goes from bad to worse.' Available at *http://www.libertycentral.org.uk/content/view/403/34* [Accessed 17 November 2006].

Lord Northesk, a Conservative peer, believes this amendment 'will potentially create a situation where the police would have to prosecute themselves' and further maintains:

> Bodies like the Serious and Organised Crime Unit (SOCA) need to do forensic hacking as part of their investigations. If they are creating hacking tools they know full well they'll be used for hacking, I will definitely be seeking to change it. The Home Office is in enough trouble already, so the thought of them enacting a law to stop the police doing their job is extraordinary.[357]

Lord Northesk tried unsuccessfully to amend this section, by proposing to remove the paragraph that makes publicly available computer tools likely to be used in a computer offence an offence.[358]

This section inserts a new section 3A into the Computer Misuse Act.[359]

1.6.4 Transitional and saving provision

This section creates transitional amendments for the Act's provisions amending the Computer Misuse Act to provide that the amendments do not apply regarding offences committed before the amendments' coming into force or acts done before then.[360]

Undeniably, this section poses a problem as it does not address the issue of 'attacks, probes, etc' that started before this Act commenced, and still continue.

---

[357] Tom Espiner 'Lord vows to fight cybercrime laws' available at http://news.zdnet.co.uk/internet/0,39020369,39271086,00.htm [Accessed 17 November 2006].
[358] See Espiner ibid. Lord Northesk had sought to propose this at the Lords Committee stage, apparently, he failed.
[359] See the Police and Justice Act s 37.
[360] See the Police and Justice Act s 38.

1.7 Concluding remarks

Despite the efforts to reform the Computer Misuse Act, perhaps having a whole Bill devoted to amending the old law would better serve the United Kingdom, rather than having only three amendments tagged on to the much larger Police and Justice Act.[361]

2. The United States

The United States has adopted cybercrime legislation at both the state and federal levels. The study below concentrates on federal legislation, both for its more general applicability and because attempting to discuss legislation adopted by the fifty states is quite beyond the scope of this paper.

The United States prosecutes computer-related crimes under:

- The Computer Fraud and Abuse Act Section 1030 of Title 18 of the United States Code of 1986 (as amended in 1994, 1996 and in 2001 by the Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT) Act of 2001).

- The Stored Communications Act of 1986 Section 2701 of Title 18 of the United States Code.

- The Fraud and Related Activity in Connection with Access-Devices Section 1029 of Title 18 of the United States Code.

- The Use of Interstate Facilities to Transmit Information about a Minor Section 2425 of Title 18 of the United States Code.

[361] The United Kingdom waited for 16 years to amend this law, and somehow three amendments seem inadequate. The Police and Justice Act contains a total of 55 sections.

- The Communications Decency Act (CDA) of 1996 Section 223 of Title 47 of the United States Code.

- The Child Online Protection Act (COPA) of 1998 Section 231 of Title 47 of the United States Code.

- The Copyright Act of 1976, as amended, Section 506 of Title 17 of the United States Code.

- The criminal infringement of a copyright Section 2319 of Title 18 of the United States Code.

2.1. The Computer Fraud and Abuse Act

The United States first enacted this law in 1986 and revised it in 1994, 1996 and in 2001 with the USA PATRIOT Act. This law intends to reduce hacking of computer systems by criminalising activities designed to access a federal or 'protected computer.'[362] Criminal offences under this Act include:

- Knowingly accessing an unauthorised computer and obtaining national security data.

- Intentionally accessing an unauthorised computer and obtaining information from any protected computer.

- Intentionally accessing any unauthorised government computer and affecting the government's use of the computer.

---

[362] See the Computer Fraud and Abuse Act of 1986 18 USC § 1030. Available at *http://www.usdoj.gov/criminal/cybercrime/1030_new.html* [Accessed 23 November 2006]. The Act defines a 'protected computer' as:

- a computer used exclusively by a financial institution or the federal government or although nonexclusively, that is used by or for a financial institution or the government and the conduct constituting the offence affects that use; or
- a computer that is used in interstate or foreign commerce or communications, including a computer outside the United States used in a way that affects interstate or foreign commerce or communication. See also 18 USC § 1030(e)(2).

- Knowingly accessing an unauthorised protected computer intending to defraud and obtaining anything of value.

- Knowingly transmitting a program, information, code or command and damaging an unauthorised protected computer, intentionally accessing an unauthorised protected computer and recklessly or otherwise causing damage.

- Knowingly and intending to defraud, trafficking in any password or similar information through which a computer may be accessed without authorisation.

- Transmitting in commerce any communication containing any threat to damage a protected computer, intentionally to extort money or other valuables.

Conviction for any offence is a fine or imprisonment for not more than ten years, or both, or a fine or imprisonment not exceeding 20 years, or both, for a subsequent conviction for another offence or its attempt.[363]

2.1.1 Knowingly accessing an unauthorised computer and obtaining national security data

This section criminalises deliberately breaking into a computer to obtain restricted information or attempting to do so.[364] It requires proof that a person used an unauthorised computer or exceeded the authority, for obtaining restricted data and thus performed some unauthorised communication or other improper act. The section prohibits the use of a computer, not the unauthorised possession or the subsequent transmission of the information.[365] As the United States Department of Justice indicates, '[e]xisting espionage laws would provide an adequate basis for the prosecution of individuals who attempt to peddle governmental secrets to foreign governments.'[366]

---

[363] See 18 USC § 1030(c)(1)(A) and (B).
[364] See 18 USC § 1030(a)(1).
[365] See the U.S. Department of Justice 'The Computer Crime and Intellectual Property Section the National Information Infrastructure Protection Act of 1996 legislative analysis.' Available at http://justice.gov/criminal/cybercrime/1030_anal.html [Accessed 23 November 2006].
[366] Ibid.

2.1.2 Intentionally accessing an unauthorised computer and obtaining information from any protected computer

This section punishes computer misuse intended to obtain information from any protected computer.[367] Essentially, it is designed to protect the confidentiality of computer data. This covers information obtained from:

- the finance authorities' financial records;
- the Government; or
- any protected computer if the conduct involves an interstate or foreign communication.[368]

The section does not merely punish the acquisition of information but proscribes intentionally accessing a computer without or exceeding the authority and subsequently obtaining information. More simply, if the information is available it must be obtained legally and not through hacking.[369]

2.1.3 Intentionally accessing any unauthorised government computer and affecting the government's use of the computer

This section prohibits accessing an authorised government computer, exclusively or non-exclusively used, when such access affects the government's use of the computer.[370] It protects a full-time or part-time government computer from outsiders regardless of whether the latter obtains any information.[371] A person not authorised to access any non-public government computer violates the integrity of a government computer by gaining unauthorised access and thus commits an offence even when not jeopardising the confidentiality of data. Simply put, any unauthorised access violates this law, even if this access is not damaging or no property is stolen. However, if the

[367] See 18 USC § 1030(a)(2).
[368] See 18 USC § 1030(a)(2).
[369] See the Computer Crime and Intellectual Property Section note 365.
[370] See 18 USC § 1030(a)(3).
[371] This section is a strict trespass provision.

government uses the computer part-time, the prosecution must show that the criminal's conduct affected the government's use of the computer.[372]

2.1.4 Knowingly accessing an unauthorised protected computer intending to defraud and obtaining anything of value

This section proscribes knowingly accessing a 'protected computer' without or exceeding authorised use, with the intention to defraud, and by such conduct furthering the intended fraud and obtaining anything of value.[373] It punishes those who use computers in schemes to defraud victims of property. This fraud provision excludes cases involving less than $5,000 of computer use in a year.[374] The term 'protected computer' is significant as it also covers private entities, thus protecting them from this criminal conduct.[375] For instance, North Bay Health Care Group (North Bay), a non-profit making organisation, brought ten counts of charges against Jessica Quitugua Sabathia, an accounts payable clerk for fraudulently using her computer to embezzle more than $875, 035. Between July 2001 and April 2004, Sabathia used her computer to access North Bay's accounting software. Unauthorised, Sabathia issued approximately 127 checks payable to herself and others. Concealing the fraud, Sabathia altered the electronic check register making it appear as if the checks had been payable to the organisation's vendors. Sabathia cashed several checks, deposited some into her bank account and some into others' bank accounts and also used some for personal expenses. Sabathia faces a maximum of five years' imprisonment, and up to a $250,000 fine for each count of the computer fraud, if convicted.[376]

---

[372] See 18 USC § 1030(a)(3).
[373] See 18 USC § 1030(a)(4).
[374] See 18 USC § 1030(a)(4).
[375] For the definition of 'protected computer' see note 362.
[376] See the United States Department of Justice 'Vallejo woman charged with embezzling more than $875,035.' Available at *http://www.cybercrime.gov/sabathiaCharged.htm* [Accessed 23 November 2006]. North Bay operates hospitals and clinics in Vacaville and Fairfield, California. See also 'Woman hacks North Bay Health Care Group.' Available at *http://www.crime-research.org/news/10.06.2004/419* [Accessed 23 November 2006].

2.1.5 Knowingly transmitting a program, information, code, or command and intentionally causing damage to an unauthorised protected computer, intentionally accessing an unauthorised protected computer and recklessly or otherwise causing damage

This section seeks to punish anyone intending to cause damage without authority, whether an outsider or an insider.[377] It creates three offences, two felonies and one misdemeanour, based on the intent and the authority of the wrongdoer. Knowingly transmitting a program, information, code, or command and intentionally causing damage to an unauthorised protected computer amounts to a felony.[378] Similarly, intentionally accessing an unauthorised protected computer and recklessly causing damage is a felony.[379] Intentionally accessing an unauthorised protected computer and incidentally causing damage amounts to a misdemeanour, as the damage caused is not intentional or reckless.[380] This section broadly defines damage as including any impairment to the integrity or availability of data, a program, a system or information resulting in:

- loss to one or more during any one-year period aggregating at least $5,000 in value;
- modifying or impairing or potentially modifying or impairing any medical record of one or more individuals;
- physical injury to any person;
- a threat to public health or safety; or
- damage affecting a government computer system.[381]

A leading case of a hacker prosecuted under this section is *United States v Morris*.[382] The defendant, Robert Morris, was a first year graduate student studying computer science at Cornell University and a son of a chief scientist at a division of the National Security Agency. The University had given Morris authorisation to use

[377] See 18 USC § 1030(a)(5). The section also covers attempts that would cause damage, if completed.
[378] See 18 USC § 1030(a)(5)(A).
[379] See 18 USC § 1030(a)(5)(B).
[380] See 18 USC § 1030(a)(5)(C).
[381] See 18 USC § 1030(e)(8).
[382] 928 F 2d 504 (2d Cir. 1991).

computers in the Computer Science Division. In October 1988, Morris created a program later to be called the INTERNET 'worm,' that would spread widely, yet draw little attention and he programmed it so that it would be difficult for other programmers to detect and therefore 'kill'. Morris launched the worm from a computer in the Massachusetts Institute of Technology in November 1988 and the worm got out of hand, actually replicating and reinfecting at a faster rate than he had anticipated. When he realised the damage being done he tried to stop the worm by sending an anonymous message over the network to warn programmers and advise them how to kill the worm and prevent reinfection. Unfortunately, his attempt failed because the network was too clogged and the warning message did not get through in time. The worm spread and affected networked computers, including government and universities' systems, causing some 6,200 computers to shut down. Labour costs to clear the software ran from approximately $96 million to $11.1 billion.

According to the experts in the field, the worm did not damage computer hardware or software, but this did not exonerate Morris from his conduct. However, Morris argued (*inter alia*) that he did not access the computers unauthorised; rather, he had exceeded his authority. The court held that he did not 'exceed authorisation' since it contended that he was totally unauthorised to access those computers into which he released the worm. Morris was expelled from Cornell, sentenced to three years' probation, 400 hours of community service, and a fine of $10,000 and the costs of his supervision. This case sets a precedent that a person who creates worms and virus can be held accountable.

Most recently, on 16 October 2006, a San Diego federal court sentenced Jay Vern Heim for recklessly damaging a protected computer.[383] Heim pleaded guilty and also admitted that he was a founding partner and former employee of Facility Automation Systems (FAS), a San Diego company installing and maintaining building automation systems.[384] Additionally, Heim admitted that on 26 January 2006, he used the username and password assigned to FAS for its Internet domain,

---

[383] See United States Department of Justice 'California man sentenced for recklessly damaging a protected computer owned by his former employer.' Available at http://www.cybercrime.gov/heimSent.htm [Accessed 23 November 2006]. Heim violated 18 USC § 1030(a)(5)(A)(ii).
[384] See ibid.

facilityautomationsystems.com, and redirected all traffic, including electronic mail, to a server at Heim's new employer, the Monero Valley Unified School District.[385] Heim redirected the traffic knowing that FAS's web site and electronic mail services would be inaccessible.[386] Lost productivity and restoring services costs exceeded $6,000. Heim was sentenced to two years' probation and fined $500 and was also required to make a $6,050 restitution to FAS.[387]

2.1.6 Knowingly and intending to defraud, trafficking in any password or similar information through which a computer may be accessed without authorisation

This section penalises anyone trafficking in passwords or similar information through which a computer may be accessed without authorisation if the trafficking affects interstate or foreign commerce or if the United States Government uses such computer.[388]

The first instance of a trespasser charged and convicted under this section was the case of Kevin David Mitnick. Mitnick was arrested in December 1988.[389] 'Mitnick was a colorful figure who went by the code name 'Condor,' was listed under the telephone directory as 'James Bond,' and had '007' as the last three digits of his telephone number.'[390] Before the conviction Mitnick had a long list of encounters with law enforcement and security officials.[391] Mitnick was charged with four counts of computer fraud under 18 U.S.C. 1030, including stealing programs valued at US$ 1 million from the Digital Equipment Corporation and using unauthorised service codes to avoid telephone charges while accessing computer systems at Leeds University in England.[392] Digital Equipment Corporation reported that reworking its software and

---

[385] See ibid.
[386] See ibid.
[387] See ibid.
[388] See 18 USC § 1030(a)(6).
[389] See, for example, Baker (note 6) at 73. See also Rotten.com 'Kevin Mitnick.' Available at http://www.rotten.com/library/bio/hackers/kevin-mitnick/ [Accessed 15 January 2007].
[390] Baker (note 6) at 73. See Christensen note 347.
[391] See, for example, Baker (note 6) at 73. See also Christensen note 347.
[392] See, for example, Baker (note 6) at 73.

repairing the damage Mitnick had caused would cost them more than US$ 4 million in downtime.[393]

Mitnick was treated as a hard-core criminal, denied bail and not allowed to make phone calls fearing that he would access other computers over the telephone lines.[394] Mitnick was severely restricted in prison and considered a high risk and danger to the public.[395] According to the authorities Mitnick could 'hack into computers using just his voice and a phone'.[396] Finally, Mitnick was sentenced to one year of imprisonment, six months in a residential treatment program and three years' probation was forbidden to use a computer or associate with other computer criminals.[397] The Justice Department considered this sentence the most severe a hacker ever received.[398]

2.1.7 Transmitting in commerce any communication containing any threat to damage a protected computer, intentionally to extort money or other valuables

This section criminalises transmitting threatening communication to damage a protected computer, intentionally to extort money or other valuables.[399] It addresses a growing problem: hackers threatening to crash systems if their demands are not met. [400] For instance, the United States Justice Department states that recently an individual threatened to crash a computer system if not allowed access and given an account.[401] In another case an individual penetrated a city government's computer system and encrypted the data on a hard drive, thus leading the victim to believe an extortion demand was impending.[402]

---

[393] See ibid.
[394] See, for example, Baker (note 6) at 73. See also Rotten.com note 389.
[395] See ibid.
[396] See, for example, Rotten.com note 389.
[397] See Rotten.com note 389. See also Baker (note 6) at 74.
[398] See Baker (note 6) at 74.
[399] See 18 USC § 1030(a)(7).
[400] See 18 USC § 1030(a)(7).
[401] See the U.S. Department of Justice note 365.
[402] See the U.S. Department of Justice ibid. The extortion demand never followed and so the victim recovered from the incident.

This section intends punishing anyone intending to extort any money or other valuables from any person transmitting in interstate or foreign commerce any communication containing any threat to damage a protected computer.[403]

2.2 The Stored Communications Act

This Act protects the privacy of stored electronic communications, either before transmitting communication or after delivery, if keeping a copy of the message.[404] These provisions target technologies such as electronic mail and computer transmissions, when keeping copies of the messages.[405] This section criminalises:

- intentionally accessing an unauthorised facility providing an electronic communication;[406]
- intentionally exceeding authority to access a facility providing an electronic communication;[407]
- and obtaining, altering or preventing authorised access to a wire or electronic communication in electronic storage.[408]

Basically, punishment for these offences is a fine, or imprisonment for not exceeding a year, or both, for a first offence, and a fine, or imprisonment for not more

---

[403] The section defines a person as any individual, firm, corporation, educational institution, financial institution, governmental entity, or legal or other entity. See 18 USC § 1030(e)(12).
[404] See the Stored Communications Act of 1986 18 USC § 2701. Available at *http://www.law.cornell.edu/uscode/uscode18/usc_sec_18_00002701----000-.html* [Accessed 18 December 2006].
[405] See the United States Department of Justice 'Criminal resource manual 1061 unlawful access to stored communications 18 U.S.C. § 2701.' Available at *http://www.usdoj.gov/usao/eousa/foia_reading_room/usam/tilte9/crm01061.htm* [Accessed 18 December 2006].
[406] See 18 USC § 2701(a)(1).
[407] See 18 USC § 2701(a)(2).
[408] See 18 USC § 2701(a). The law defines 'electronic storage' as both any temporary, intermediate storage of a wire or electronic communication incidental to the electronic transmission thereof and the storage of such communication by an electronic communication service for purposes of backup protection of such communication. See also the Definitions 18 USC § 2510(17) available at *http://www.law.cornell.edu/uscode/18/usc_sec_18_00002510----000-.html* [Accessed 18 December 2006].

than five years, or both, for a subsequent offence.[409] However, penalties increase if the offence was committed for commercial gain or malicious damage. In such cases the imprisonment term increases by not more than five years for a first offence, and by not more than ten years for a subsequent offence.[410]

2.3 The Fraud and Related Activity in Connection with Access-Devices

This section criminalises fraud and related activities connected with access devices if the offence affects the interstate or foreign commerce.[411] It outlaws:

- Knowingly and intending to defraud producing, using or trafficking in a counterfeit access device.[412]

- Knowingly and intending to defraud trafficking in or using an unauthorised device during any one-year period and obtaining anything of a value aggregating at least $1,000.[413]

- Knowingly and intending to defraud possessing fifteen or more counterfeit devices or unauthorised access devices.[414]

- Knowingly and intending to defraud producing, trafficking in or possessing access device-making equipment.[415]

---

[409] See 18 USC § 2701(b)(2).
[410] See 18 USC § 2701(b)(1).
[411] See the Fraud and Related Activity in Connection with Access-Devices 18 USC § 1029. Available at *http://www4.law.cornell.edu/uscode/html/uscode18/usc_sec_18_00001029----000-.html* [Accessed 5 December 2006]. The section defines 'access device' as any card, plate, code, account number, electronic serial number, mobile identification number, personal identification number, or other telecommunications service, equipment, or instrument identifier, or other means of account access that can be used, alone or in conjunction with another access device, to obtain money, goods, services, or any other thing of value, or that can be used to initiate a transfer of funds (other than a transfer originated solely by paper instrument). See also 18 USC § 1029(e)(1).
[412] See 18 USC § 1029(a)(1).
[413] See 18 USC § 1029(a)(2).
[414] See 18 USC § 1029(a)(3).
[415] See 18 USC § 1029(a)(4).

- Knowingly and intending to defraud transacting with an access device issued to any person to receive anything of value during any one-year period valued at not less than $1,000.[416]

- Knowingly and intending to defraud soliciting for offering an access device, or selling information regarding or applying to obtain an access device, without the issuer of the access device's authorisation.[417]

- Knowingly and intending to defraud using, producing, trafficking in or possessing a telecommunications instrument modified or altered to obtain unauthorised use of telecommunications services.[418]

- Knowingly and intending to defraud using, producing, trafficking in or possessing a scanning receiver.[419]

- Knowingly using, producing, trafficking in or possessing hardware or software knowing it has been configured to modify telecommunications identifying information associated with a telecommunications instrument; to use the instrument to obtain unauthorised telecommunications service.[420]

- Knowingly and intending to defraud arranging for a person to present an access device's transactions record to the owner for payment, without a credit card owner's authorisation.[421]

The offence is punishable by a fine or imprisonment for a period not exceeding 15 years, or both, for a first offence, and a fine or imprisonment for not more than 20 years, or both, for a subsequent offence.[422]

---

[416] See 18 USC § 1029(a)(5).
[417] See 18 USC § 1029(a)(6).
[418] See 18 USC § 1029(a)(7).
[419] See 18 USC § 1029(a)(8).
[420] See 18 USC § 1029(a)(9).
[421] See 18 USC § 1029(a)(10).
[422] See 18 USC § 1029(c).

2.4 The Use of Interstate Facilities to Transmit Information about a Minor

This section proscribes using the mail or any interstate or foreign commerce facility, or using the mail or a facility within the special maritime and territorial jurisdiction of the United States to transmit information about a minor.[423] It criminalises:

- Knowingly initiating to transmit a person's details knowing that person to be below the age of 16 years, intending to entice, encourage, offer or solicit any person to engage in sexual activity for which any person can be criminally liable.[424]

- Any attempt to violate this law.[425]

Upon conviction, a person is liable to a fine, or imprisonment not exceeding five years, or both.[426]

2.5 The Communications Decency Act

This section criminalises the use of a telecommunications device in interstate or foreign communications for obscene or harassing communications.[427]

2.5.1 Prohibited acts generally

This section prohibits:

- Making, or soliciting and initiating to transmit any obscene communication or child pornography, intending to annoy, abuse, threaten or harass another person.[428]

[423] See the Use Interstate Facilities to Transmit Information about a Minor 18 USC § 2425. Available at *http://www.law.cornell.edu/uscode/18/usc_sec_18_00002425----000-.html* [Accessed 5 December 2006].
[424] See 18 USC § 2425.
[425] See 18 USC § 2425.
[426] See 18 USC § 2425.
[427] See the Communications Decency Act of 1996 47 USC § 223. Available at *http://www.cybertelecom.org/cda/cda.htm* [Accessed 5 December 2006].

- Making, or soliciting and initiating to transmit any obscene communication or child pornography knowing the communication's recipient to be under 18 years, disregarding whether the communication's maker placed the call or initiated the communication.[429]

- Calling or utilising a telecommunications device without disclosing identity and intending to annoy, abuse, threaten or harass any person at the receiving end, disregarding whether conversation or communication ensues.[430]

- Repeatedly ringing a telephone number intending to harass any person at the receiving end.[431]

- Repeatedly calling or initiating communication with a telecommunications device during which communication ensues solely to harass any person at the receiving end.[432]

- Knowing permitting any telecommunications facility under own control to be used in committing any criminal offence under this section.[433]

These offences are punishable by a fine, or a maximum imprisonment of two years, or both.[434]

2.5.2 Prohibited acts for commercial purposes

This section criminalises:

---

[428] See 47 USC § 223(a)(1)(A).
[429] See 47 USC § 223(a)(1)(B).
[430] See 47 USC § 223(a)(1)(C).
[431] See 47 USC § 223(a)(1)(D).
[432] See 47 USC § 223(a)(1)(E).
[433] See 47 USC § 223(a)(2).
[434] See 47 USC § 223(a).

- Knowingly using a telephone, within the United States, to make an obscene communication for commercial purposes or allowing a telephone under one's own control to be used for this purpose;[435] or

- Knowingly using a telephone, within the United States, available to anyone below 18 years or to anyone without consent to make an indecent communication for commercial purposes, disregarding whether the communication's maker placed the call, or allowing a telephone facility under one's own control to be used for this purpose.[436]

Conviction is punishable by a fine or a maximum imprisonment of two years, or both.[437]

2.6 The Child Online Protection Act

This law criminalises knowingly availing any harmful material to minors for commercial purposes 'by means of the World Wide Web,' in interstate or foreign commerce, unless the person has restricted access to minors.[438]

The offence is punishable by a fine or imprisonment not exceeding six months, or both.[439] Further, anyone intentionally violating this law is additionally liable to a

---

[435] See 47 USC § 223(b)(1).
[436] See 47 USC § 223(b)(2).
[437] See 47 USC § 223(b)(1) and (b)(2)(B).
[438] See the Child Online Protection Act of 1998 47 USC § 231(a)(1). Available at *http://www4.law.cornell.edu/uscode/html/uscode47/usc_sec_47_00000231----000-.html* [Accessed 5 December 2006]. The Act defines the term 'by means of the World Wide Web' as by placement of material in a computer server-based file archive so that it is publicly accessible, over the Internet, using hypertext transfer protocol or any successor protocol. It also defines the term 'material that is harmful to minors' as communication, picture, image, graphic image file, article, recording, writing, or other matter of any kind that is obscene or that:
- the average person, applying contemporary community standards, would find, taking the material as a whole and with respect to minors, is designed to appeal to, or is designed to pander to, the prurient interest;
- depicts, describes, or represents, in a manner patently offensive with respect to minors, an actual or simulated sexual act or sexual contact, an actual or simulated normal or perverted sexual act, or a lewd exhibition of the genitals or post-pubescent female breast; and
- taken as a whole, lacks serious literary, artistic, political, or scientific value for minors.

See also 47 USC § 231(e)(1) and (e)(6), respectively. Further, see 47 USC § 231(c)(1).
[439] See 47 USC § 231(a)(1).

fine not exceeding $50,000 for each violation and a further civil penalty not exceeding the same amount for each violation.[440]

2.7 The Copyright Act

This statute creates copyright infringement for unlawfully reproducing and distributing copyright including by electronic means.[441] The criminal infringement statute has three elements:

- infringement of a copyright;
- done wilfully; and
- for commercial or private benefits.[442]

Punishment for this offence is a fine, or imprisonment for a maximum of five years, or both, for a first offence, if consisting of reproducing or distributing at least ten copies or phonorecords of a copyrighted work, valued at not less than $2,500.[443] Punishment for a subsequent offence is a fine, or imprisonment for a period not exceeding ten years, or both.[444] However, in any other case, punishment for this offence is a fine, or imprisonment for not more than one year, or both.[445]

2.8 Concerns

Although, the United States' cybercrime laws are apparently comprehensive, there are some concerns:

---

[440] See 47 USC 231(a)(2) and (3). According to these subsections each day of violation constitutes a separate offence.
[441] See the Copyright Act of 1976 (as amended) 17 USC § 501(a). Available at *http://www.law.cornell.edu/copyright/copyright.act.chapt5.html* [Accessed 6 December 2006]. 'Copyright infringement' broadly refers to the unauthorised use of protected material by intellectual property rights particularly the copyright violating the original copyright owner's exclusive rights, such as the right to reproduce or distribute the copyrighted work.
[442] See 17 USC § 506-(a). Anyone violating this law is criminally liable in addition to any other provisions of any other law. See 18 USC § 2319-(a). Available at *http://www.usdoj.gov/criminal/cybercrime/18usc2319.htm* [Accessed 18 December 2006].
[443] See 18 USC § 2319(b)(1).
[444] See 18 USC § 2319(b)(2).
[445] See 18 USC § 2319(b)(3).

- The United States cybercrime laws are dispersed in too many different pieces of legislation, which means that securing convictions may sometimes be difficult for lack of identifying the relevant law.

- The United States tends to pass severe and restrictive cybercrime laws that place unacceptably heavy burdens on legally protected speech, and are thus unconstitutional. Thus, in *Reno v American Civil Liberties Union*[446] the Supreme Court invalidated portions of the Communications Decency Act regarding 'indecent' communication by a telecommunication device and 'patently offensive' communications through use of interactive computer service to minors. The court struck down these provisions intended to protect children from indecent speech as unconstitutional, for infringing the First Amendment right to free speech and for not allowing parents to decide on what was acceptable material for their children. Further, the court stated that the provisions extended to non-commercial speech and did not define 'patently offensive', a term legally undefined. Likewise, the Child Online Protection Act (COPA) overly restricts adults from legally accessible Internet sites. According to the Center for Democracy and Technology 'COPA places unconstitutional burdens on a wide category of protected speech, while failing to achieve its goal of protecting children.'[447] Hence, in 1998, in *Ashcroft v American Civil Liberties Union*[448] the district court granted a temporary restraining order against this law. Again, in 2002, the Supreme Court confirmed the lower court decision enjoining Internet pornography law because it would overly restrict adults from legally accessible Internet sites.[449]

- The United States actively participated in drafting the Council of Europe Convention on Cybercrime; this was generally unwelcome, the American public viewed the drafting as secret until the public release of draft 19 in 2000.[450]

---

[446] 521 U.S. 844 (1997).
[447] See the Center for Democracy and Technology 'Child Online Protection Act (COPA).' Available at http://www.cdt.org/speech/copa/ [Accessed 5 December 2006].
[448] 532 U.S. 1037, 121 S. Ct 1997 (2001).
[449] See *Ashcroft v Free Speech Coalition* 535 U.S. 234 (2002).
[450] See Mike Godwin 'Watch out: an international treaty on cybercrime sounds like a great idea, until you read the fine print.' Available at http://cryptome.org/cycrime-godwin.htm [Accessed 5 December 2006]. Although the United States is not a member of the Council of Europe, it participated in drafting the Convention as an 'observer'. It accepted the invitation and was active in the Convention's drafting through the Department of Justice. The Convention was adopted by the Council on 8 November 2001

However, the Justice Department responded that it made several presentations and met with stakeholders in negotiating the Convention.[451] Actually, the American public had many reservations about the Convention, arguing that the Convention threatens their core civil liberties protections by:

- failing 'to provide meaningful privacy and civil liberties protections' and being too broad in defining crimes and covering much more than computer-related crimes;[452]
- lacking a 'dual criminality' provision providing that an activity must be a criminal offence in both countries before one country can demand cooperation from another.[453] This would require the United States law enforcement officials to co-operate with a foreign police force in investigating an activity that, while criminal in their jurisdiction, is perfectly legal in the United States.[454] Additionally, the Convention places a large burden on the business industry to assist law enforcement in investigations.[455] As a result, businesses worry that the Convention provisions would increase costs to service providers, and hinder the development of security technologies and the sale of encryption programs, thus negatively impacting on e-commerce;[456] and
- supporting the ratification of the Convention despite no major European country having ratified the Convention.[457] The American public considered this to be an attempt by the government 'to obtain more power than it could obtain with the USA PATRIOT Act after September11, 2001.'[458] To fully attain its purpose in effectively deterring cybercrime, more states will have to sign the Convention and abide by its provisions.[459] To bind the United States, the Convention requires the approval of two-thirds of the Senate.[460]

---

and signed by the United States on 23 November 2001. See 2.5 Chap 2 above. See also the FAQs on the Convention note 238.

[451] See Godwin note 450.

[452] See the Electronic Privacy Information Center (hereinafter, 'EPIC') 'The Council of Europe's Convention on Cybercrime.' Available at *http://www.epic.org/privacy/intl/ccc.html#summary* [Accessed 22 August 2006].

[453] Ibid.

[454] See the EPIC ibid. See also Godwin note 450.

[455] See the Convention (note 166) Art 18(1)

[456] See the FAQs note 238.

[457] Although 30 countries participated in signing the Convention in November 2001, the only major European country which ratified the Convention is France in 2006. See the Convention on Cybercrime CETS No.: 185 note 237.

[458] See EPIC note 452.

[459] See FAQs note 238.

[460] See Godwin note 450.

> '[W]hether senators decide that the need to combat cybercrimes trumps concerns about submitting U.S. citizens and companies to foreign criminal process remains an open question.'[461]

2.9 Concluding remarks

Generally, the United States has comprehensive legislation governing cybercrime; it criminalises nine out of ten types of cybercrimes and the country also has severe penalties for this crime.[462]

Responding generally to the Americans' sentiments towards the Convention, the Department of Justice explains that its delegation 'worked hard to balance attentiveness to the suggestions of other countries with respect for the strengths of current U.S. law. As a result, the central provisions of the Convention are consistent with the existing framework of U.S. law and procedure.'[463] On 29 September 2006 the United States became a party to the Council of Europe Convention on Cybercrime. The Convention entered into force for the United States on 1 January 2007.[464] The Department of Justice explains that 'the Convention is in full accord with all U.S. constitutional protections, such as free speech and other civil liberties, and will require no change to U.S. laws.'[465] The United States also urges all states to consider joining the Convention.[466]

---

[461] See Godwin note 450. The United States' sentiments towards the Convention are generally applicable to all countries.
[462] See McConnell International note 1.
[463] See FAQs note 238. See also Brenner (note 67) 34-35.
[464] See the United States Department of State 'Council of Europe Convention on Cybercrime' (29 September 2006). Available at http://www.state.gov/r/pa/prs/ps/2006/73354.htm [Accessed 23 November 2006]. On 22 September 2006, the United States President signed the instrument of ratification for the Convention and on 29 September 2006 the country became a party to the Convention upon deposit of ratification at the headquarters of the Council of Europe in Strasbourg, France.
[465] The Department of Justice 'Statement of Attorney General Alberto R Gonzales on the passage of the Cybercrime Convention' (4 August 2006). Available at http://www.usdoj.gov/opa/pr/2006/August/06_ag_499.html [Accessed 23 November 2006].
[466] The U.S. Department of State note 237.

3. South Africa

South Africa regulates cybercrime under:

- The Electronic Communications and Transactions Act 25 of 2002.
- The Regulation of Interception of Communications and Provision of Communications-Related Information Act 70 of 2002.
- The Films and Publications Act 65 of 1996 as amended by the Films and Publications Amendment Act 34 of 1999 and Act 18 of 2004.
- The Copyright Act 98 of 1978 as amended by the Copyright Amendment Act 56 of 1980, 66 of 1983, 52 of 1984, 39 of 1986, 13 of 1988, 61 of 1989, 125 of 1992, the Intellectual Property Amendment Laws 38 of 1997 and the Copyright Amendment Act of 9 of 2002.

3.1 The Electronic Communications and Transactions Act

The ECTA resulted from the South African Law Reform Commission's democratic and consultative investigation of computer crime, from 1999 until 2002, when the law was enacted.[467] Mainly, the Act aims to facilitate e-commerce by creating legal certainty and promoting confidence in electronic transactions, and addresses cybercrime in Chapter XIII.[468]

This chapter introduces the following statutory criminal offences related to information systems, the first in South African jurisprudence:

- Unauthorised access to and interception of data

[467] See the South African Law Reform Commission issue paper 14. Available at http://www.doj.gov.za/salrc/papers.htm [Accessed 24 November 2006]. See also the ECTA note 318. The ECTA has been operating since 2 August 2002.
[468] See the ECTA note 318, particularly, Chap XIII.

- Interference with data
- Computer-related extortion
- Computer-related fraud and forgery
- Attempt, and aiding and abetting

3.1.1 Unauthorised access to and interception of data

Subject to the Regulation of Interception of Communications and Provision of Communications-related Information Act 70 of 2002, this section criminalises intentionally accessing or intercepting any data without authority.[469] This section makes hackers and crackers criminally liable.[470]

3.1.2 Interference with data

This section proscribes intentionally interfering with data by modifying, destroying or otherwise rendering the data ineffective.[471] For example, a person distributing a virus programme commits this offence. Further, this offence includes the trafficking or possession of passwords or security-overriding devices to intentionally interfere with data.[472] It also includes the actual use of security overriding devices and denial of service attacks.[473]

3.1.3 Computer-related extortion

This section criminalises the unauthorised accessing, intercepting or interfering with data or threatening to do so for obtaining unlawful proprietary advantage by

---

[469] See the ECTA s 86(1). The Regulation of Interception of Communications and Provision of Communications-related Information Act 70 of 2002 (hereinafter, 'RICPIC') repeals the Interception and Monitoring Prohibition Act 127 of 1992 contained in this section. The ECTA defines 'access' as accessing data and continuing to do so after noting that such access is unauthorised. However, the Act does not define 'unauthorised'. See also the ECTA s 85. Further, see the RICPIC available at *http://www.info.gov.za/gazette/acts/2002/a70-02.pdf* [Accessed 24 November 2006].
[470] See the discussion of hacking and cracking at 2.3.2 Chap one above.
[471] See the ECTA s 86(2).
[472] See the ECTA s 86(3).
[473] See the ECTA s 86(4) and (5).

undertaking to cease such action, or by undertaking to restore any damage these actions caused.[474]

3.1.4 Computer-related fraud and forgery

This section prohibits intentionally accessing, intercepting or interfering with data for obtaining any unlawful advantage by faking data with the intent that it be considered or acted upon as if it were authentic.[475]

3.1.5 Attempt, and aiding and abetting

The Act allows for degrees of participation in any offence to be criminalised. Therefore, an attempt to commit any criminal offence prohibited under this chapter amounts to a criminal offence.[476] Further, the Act also prohibits the aiding and abetting of any person committing these criminal offences.[477]

The ECTA also regulates the sending of unsolicited commercial e-mail messages, known as 'spam.' The Act provides that the sending of such mail must allow the consumer an option to cancel subscription to that mailing list and give the identifying particulars of the provider of the consumer's personal details, upon the consumer's request.[478] Failing to comply or continuing to send the unwanted e-mails constitutes a criminal offence.[479] Further, the Act outlaws any agreement that could be implied by the consumer's failure to respond to spam.[480]

The Act punishes all these offences by a fine or a maximum imprisonment of five years.[481]

---

[474] See the ECTA s 87(1). This is the traditional 'blackmail' or extortion.
[475] See the ECTA s 87(2). This amounts to fraud, or the specialized form of fraud known as 'forgery and uttering.'
[476] See the ECTA s 88(1). The prohibited offences are those referred to in ss 86 and 87.
[477] See the ECTA s 88(2). This section takes care of accomplices to cybercrime.
[478] See the ECTA s 45(1).
[479] See the ECTA ss 45(3) and (4).
[480] See the ECTA s 45(2).
[481] See the ECTA s 89.

3.2 The Regulation of Interception of Communications and Provision of Communications-related Information Act

Under this Act, unlawfully intercepting or attempting to intercept communication to obtain confidential information is a criminal offence, except for those enforcing the law. This law extends to communications over the Internet.[482]

Conviction is punishable by a fine not exceeding R2 000 000, or imprisonment for not more than ten years.[483]

3.3 The Films and Publications Act

This Act provides for the classification of certain films and publication not suitable for persons below 18 years of age and for the registration of Internet service providers, obliging service providers to take reasonable steps to prevent distributing child pornography.[484] Further, this Act prohibits possessing, producing, procuring, accessing and distributing child pornography and distributing restricted harmful material.[485] This also covers activities committed over the Internet.[486] Thus, anyone possessing, producing, accessing and distributing child pornography, distributing restricted harmful material and not meeting the Internet service providers' obligations commits an offence.[487]

Conviction for this offence is a fine, or imprisonment for not more than ten years, or both.[488]

---

[482] See the RICPIC s 49.
[483] See the RICPIC Act s 51(1)(b)(i).
[484] See the Films and Publication Act 65 of 1996 as amended by the Films and Publication Amendment Act 34 of 1999 and 18 of 2004 ss 2 and 27A. Available at *http://www.info.gov.za/acts/1996/a65-96.pdf* [Accessed 24 November 2006].
[485] See the Films and Publication Act ss27 and 28. Restricted harmful material includes:
- explicit sexual content not suitable for children (The South African Constitution of 1996 defines 'children' as anyone below the age of 18).
- bestiality; and
- violent sexual content and extreme violence that might induce causing harm. See the Films and Publications Act schs 1 and 2.

[486] See the Films and Publication Act s 2(a)(i).
[487] See the Films and Publication Act ss 27, 27A and 28.
[488] See the Films and Publication Act ss 30(1) and (1A).

3.4 The Copyright Act

This Act creates copyright infringement for unlawfully importing, selling, letting, offering for selling or hiring, distributing copyright or acquiring an article relating to a computer program, thus criminalising:

- infringing a copyright;
- not being the owner of copyright, and acting without the owner's licence; and
- committing the offence for commercial benefits, except for acquiring a computer program (which does not include the commercial benefits requirement).[489]

Upon a first conviction a person is liable to a fine not exceeding R5 000, or imprisonment for not more than three years, or both, for each article to which the offence relates.[490] Subsequently, for each article to which the offence relates, a person is liable to a fine not exceeding R10 000, or imprisonment for up to five years, or both. [491]

3.5 Concerns

As commendable as the Law Commission's efforts are, as seen by the birth of the ECTA, the law still has some loopholes:

- Although the ECTA defines 'access', it does not attempt to define 'unauthorised'; as a result, the law is unclear regarding what constitutes 'unauthorised' access.

- The Act does not address 'theft of information' over the Internet. This issue is still very thorny, computer-related or not. Undeniably, information is an intangible object, and thus, according to the law an object must be tangible before being

[489] See the Copyright Act 98 of 1978 as amended by the Copyright Amendment Act 56 of 1980, 66 of 1983, 52 of 1984, 39 of 1986, 13 of 1988, 61 of 1989, 125 of 1992, the Intellectual Property Amendment Laws 38 of 1997 and the Copyright Amendment Act of 9 of 2002 ss 23(a)-(c) read with s 11B available at *http://www.gpa.co.za/pdf/legislation/Copyright%20Act.pdf* [Accessed 9 January 2007].
[490] See the Copyright Act s 27(6)(a).
[491] See the Copyright Act s 27(6)(b).

stolen. Consequently, theft of information cannot amount to theft. However, this argument is yet to be addressed by the court. The South African Law Reform Commission is currently considering criminalising this conduct.[492]

- The penalties are too light given how much cybercrime causes; the damage far exceeds the punishment.

- Cybercrime is a serious offence that must be treated on its own; merely addressing it in one chapter is hardly giving it the attention it deserves.

3.6 Concluding remarks

According to South African law 'in instances where there is a lack of law in a specific area, reference to international jurisdictions is permissible.'[493] Moreover, South Africa is a signatory of the Council of Europe Convention on Cybercrime.[494] This allows South Africa to borrow from other countries and the Convention. Consequently, South Africa may prosecute all types of cybercrimes on the basis of permissibility however; this is yet to be tested in the courts of law.

4. Conclusion

This chapter investigating the cybercrime legislation of three countries, the United Kingdom, the United States and South Africa, shows initiatives in reforming legal systems to address cybercrime. Whilst these countries' laws may not be perfect and water-tight, they demonstrate a positive commitment to the fight against cybercrime.

---

[492] See the South African Law Reform Commission 'Discussion paper 109' (October 2005). Available at http://www.doj.gov.za/salrc/dpapers.htm [Accessed 8 February 2007].
[493] Reinhardt Buys (ed) *Cyberlaw @ SA top 100 FAQs* virtualbook 294.
[494] South Africa is one of the four countries that participated 'as observers' in negotiating the Convention on Cybercrime. See, for example, FAQs note 238 and the Convention on Cybercrime CETS No.:185 note 237.

CHAPTER FOUR: CYBERCRIME LEGISLATION FOR LESOTHO

Overview

As criminals take their criminal activities to new heights in the electronic age and having identified Lesotho's current laws' shortcomings regarding cybercrime, (we can conclude that) Lesotho is urged to (must) seriously consider adopting cybercrime legislation.[495] However, the difficulty lies in establishing a well defined rule of law to find and prosecute cybercriminals. This chapter examines the approach that Lesotho can take in developing a comprehensive legal framework addressing cybercrime.

1. Cybercrime model law for Lesotho

Lesotho needs a clearly defined rule of law including a strong deterrent for cybercrime, to effectively protect valuable information and systems and people generally, so that Lesotho's citizens can truly enjoy the digital age's benefits. Countries embarking on the introduction of cybercrime laws seek a model to follow. Lesotho is likely to succeed in developing a comprehensive legal structure combating cybercrime because of the existing international and supranational initiatives providing guidance for an effective framework addressing this crime.[496] Further, Lesotho has the added advantage of learning and borrowing from the experiences of her sister countries (such as the United Kingdom, the United States and South Africa) that have already enacted cybercrime laws.[497]

In developing a legal framework addressing cybercrime Lesotho must legislate on:

---

[495] See 1.1 Chap one above.
[496] See generally Chap two above.
[497] See generally Chap three above.

- Substantive criminal law
- Procedural law
- Mutual legal assistance agreements

1.1 Substantive criminal law

To prosecute cybercrime, Lesotho must harmonise substantive offences, by:

- creating a new law specifically targeting cybercrime;
- amending old laws to encompass the use of computer technology in committing conventional offences; and
- establishing ancillary liability and sanctions.

1.1.1 Creating a new law

Creating a new law is absolutely necessary to address crimes that Lesotho does not comprehensively address. These are offences committed against the confidentiality, integrity and availability of computer data and systems, crimes that never existed before the advent of computers.[498] To address the most serious cybercrimes, Lesotho must criminalise:

- Illegal access
- Illegal interception
- Data interference
- System interference
- Misuse of devices[499]

[498] See 2.2.1 Chap one above.
[499] The international and supranational initiatives in chapter two above provide a minimal listing of conduct that States must criminalise to address the most serious cybercrime. Particularly, see the Convention (note 168) Art 2-6. See also Schjolberg (note 56) 11.

Illegal access

Lesotho must prohibit intentionally accessing the whole or any part of a computer system, without the right to do so, or the unauthorised access to data.[500] Illegal access to computer systems and networks is 'computer trespass,' 'cracking' or 'hacking' offences; merely activating the computer security devices constitutes an offence, regardless of whether access to the data is obtained.[501] Basically, illegal access dangerously threatens and attacks the security (the confidentiality, integrity and availability) of computer systems and data.[502] This provision allows organisations and individuals to operate their systems in an undisturbed and uninhibited manner.[503] Access requires entering another computer system or network.[504] For some States like the United States and South Africa, merely accessing a computer system is not an offence; they additionally require obtaining information.[505] Thus, an offence is committed when a person intentionally and without authority obtains access to stored data. Generally, ''[o]btaining information' includes the mere observation and reading of the information, i.e. there is no requirement that the information has to be downloaded.'[506] In contrast, the United Kingdom does not require the obtaining of any information, merely accessing any program or data constitutes an offence.[507]

Like the United Kingdom, Lesotho can take the wide approach and criminalise mere hacking.[508] Alternatively, Lesotho can criminalise this conduct by attaching qualifying elements, such as infringing security measures, special intent to obtain computer data or other dishonest intent, or relating to a computer system that is connected to another computer system.[509] Requiring that the offence be committed relating to a computer connected to another computer system will allow Lesotho to

---

[500] See the Convention (note 166) Art 2.
[501] See Schjolberg (note 56) 11. Basically, 'computer trespass' is the unauthorized intrusion, the 'hacking' or 'cracking' of a computer system. For the definition of 'hacking' and 'cracking' see the discussion of hacking and cracking at 2.3.2 Chap one above.
[502] See the Explanatory Report (note 221) para 44.
[503] See ibid.
[504] See ibid para 46.
[505] See 18 USC § 1030(a)(2)(C), the ECTA s 86(1), respectively. See also 2.1.1 and 3.1.1 Chap three above, respectively.
[506] Schjolberg (note 56) 11.
[507] See the Computer Misuse Act s 1. See also 1.2.1 Chap three above.
[508] See the Computer Misuse Act s 1. See also 1.2.1 Chap three above.
[509] See the Convention (note 166) Art 2. Lesotho may follow the United States and South Africa's narrower approach.

exclude a person accessing a stand-alone computer without any use of another computer system.[510] Lesotho may restrict the offence to illegal access to networked computer systems (including telecommunication services, public networks and private networks, such as Intranets and Extranets).[511]

Illegal interception

Lesotho must proscribe intentionally intercepting non-public transmissions of computer data, including electromagnetic emissions, to, from or within a computer system, by technical means.[512] This provision aims to protect the right to privacy in data communications.[513] States worldwide protect the right to privacy in data communications differently and in different degrees.[514] For instance, South Africa punishes unlawfully intercepting communication to obtain confidential information, except for enforcing the law and, further, criminalises intercepting any data without authority.[515] Similarly, the United States protects the privacy of stored electronic communications and criminalises intentionally accessing an unauthorised facility or exceeding authority to access a facility providing an electronic communication and obtaining access to such communication.[516] On the other hand, the United Kingdom does not address this conduct.[517] Accordingly, Lesotho must protect her citizens' right to privacy in electronic communications, without over-criminalising; service providers monitoring traffic on their own networks and the protection of their rights and obligations and property must not be regarded as illegal interception.[518] The conduct is equivalent to the traditional tapping and recording of oral telephone communications. Indeed, Lesotho traditionally protects the right to privacy of communications.[519]

---

[510] See the Explanatory Report (note 221) para 50.
[511] Ibid.
[512] See the Convention (note 166) Art 3.
[513] See the Explanatory Report (note 221) para 51.
[514] See Schjolberg (note 56) 11.
[515] See the RICPIC s 49 and the ECTA s 86(1), respectively. See also 3.2 and 3.1.1 Chap three above, respectively.
[516] See 18 USC § 2701. See also 2.2 Chap three above.
[517] See Figure 1 Chap three above.
[518] See Schjolberg (note 56) 11.
[519] See the Lesotho Telecommunications Authority Act 5 of 2000 s 57. Available at *http://www.lta.org.ls/Instruments/LTA-ACT-2000.pdf* [Accessed 17 January 2007]. Save for criminal investigations, intercepting, modifying or interfering with a message sent telephonically is an offence. See also the Lesotho Telecommunications Authority Regulations 34 of 2001 s 32. The right to privacy

The offence must cover all categories of electronic communication, by telecommunication, e-mail or file transfer.[520] Further, the offence must include monitoring, surveillance, listening to the content of communications and obtaining the content of data either directly, through access and use of the computer system, or indirectly, through the use of electronic eavesdropping or tapping devices.[521] Interception may also include recording.[522] The offence requires technical means, to avoid over-criminalising.[523] Technical means includes all kinds of technical devices, namely, computer programmes, passwords and codes.[524]

The offence covers 'non-public' transmissions of computer data, qualifying the nature of the transmission process and not the nature of the data transmitted.[525] Despite the data communicated being publicly available, if parties wish to communicate confidentially, the communication is 'non-public.'[526] Similarly, if the transmission is unavailable until paid for, as in Pay-TV, the signal is 'non-public.'[527]

For consistency of prohibiting and applying the law, if Lesotho requires committing the offence with dishonest intent, or relating to a computer system that is connected to another computer system for illegal access, similar qualifying elements must also be required to attach criminal liability to this offence.[528] The mental element is crucial for criminal liability regarding illegal interception, thus Lesotho must require that the offence be committed 'intentionally' and 'without right.'[529]

---

of communications emanates from the country's supreme law, the Constitution, which protects fundamental rights and freedoms. Further, see the Lesotho Constitution of 1993 s 11. Available at http://www.parliament.ls/documents/constitution.php [Accessed 5 January 2007).

[520] See Schjolberg (note 56) 11.
[521] See the Explanatory Report (note 221) para 53.
[522] See ibid.
[523] See ibid.
[524] See ibid.
[525] See ibid para 54.
[526] See ibid.
[527] See ibid.
[528] See ibid para 59.
[529] See the Convention (note 166) Art 3.

Data interference

Lesotho must criminalise intentionally damaging, deleting, deteriorating, altering or suppressing computer data without right.[530] This provision provides computer data and programs with protections similar to tangible objects, hence protecting the integrity, availability and the proper functioning or use of stored data or computer programs.[531]

'Damaging' and 'deteriorating' are overlapping forms of conduct, rendering the content of data and programs useless or meaningless.[532] Deleting data is equal to destroying a tangible object, and occurs by obliterating data and programs from the original or previous legal appearance in their formalised manner.[533] 'Deleting' destroys and makes data unreadable, even if the data can be restored after the attack.[534] 'Altering' requires modifying the existing data, even if the data remains understandable after the attack.[535] Examples include defacing the website, introducing malicious codes and adding data without deleting, thus changing the existing data. 'Suppressing' covers activities preventing or terminating the availability of the data to the person legally entitled to the data, for instance, when causing the computer data to disappear without being deleted.[536]

This conduct does not cover common activities for designing networks or common operating or commercial practices like testing or protecting the security of systems.[537] Likewise, modifying traffic data to facilitate anonymous communications (such as anonymous remailer systems activities) or modifying data to secure communications (such as encryption) are not 'without right' and therefore are not data interference.[538] However, Lesotho may criminalise certain abuses regarding

[530] See the Convention (note 166) Art 4.
[531] See the explanatory Report (note 221) para 60.
[532] See the Explanatory Report (note 221) para 61. See also Schjolberg (note 56) 12.
[533] See the Explanatory Report (note 221) para 61.
[534] See ibid.
[535] See ibid.
[536] See ibid.
[537] See ibid para 62.
[538] See ibid.

anonymous communications, such as altering the packet header information to conceal the perpetrator's identity in committing a crime.[539]

Countries around the world respond to conduct differently. For example, the United States addresses this conduct by criminalising intentionally accessing an unauthorised facility or exceeding authority to access a facility providing an electronic communication and altering or preventing authorised access to such communication.[540] On the other hand, South Africa punishes intentionally interfering with data by modifying, destroying or otherwise rendering the data ineffective.[541] At another extreme, the United Kingdom generally outlaws unauthorised acts with intent to impair operation of a computer.[542]

For clarity and simplicity, unlike the above countries, Lesotho can merely criminalise intentionally damaging, deleting, deteriorating, altering or suppressing computer data without right. Moreover, Lesotho may require that an offence be committed when the conduct results in serious harm; interpreting what constitutes such serious harm is entirely up to Lesotho.[543]

System interference

Lesotho must prohibit serious intentional hindering of the functioning of a computer system by inputting, transmitting, damaging, deleting, deteriorating, altering, or suppressing computer data.[544] This provision aims to criminalise intentionally hindering the lawful use of computer systems, including telecommunication facilities, by interfering with computer data, thus protecting the interest of operators and users of computer or telecommunications systems for their proper functioning.[545]

---

[539] See ibid.
[540] See 18 UCS § 2701. See also 2.2 Chap three above.
[541] See the ECTA s 86(2). See also 3.1.2 Chap three at above.
[542] See the Police and Justice Act s 36. See also 1.4.2 Chap three above.
[543] See the Convention (note 166) Art 4(2). See also the Explanatory Report (note 221) para 64.
[544] See the Convention (note 166) Art 5.
[545] See the Explanatory Report (note 221) para 65. Hindering refers to activities interfering with the proper functioning of the computer system, such as, imputing, transmitting, damaging, deleting, deteriorating, altering, or suppressing computer data.

Hindering the functioning of computer systems is critical; for instance, hindering the functioning of essential services computer systems may have grave implications for society.[546] Thus, for example, targeting critical infrastructures like energy, broadcasting, transportation and telecommunications may disturb and significantly threaten public administration and society.[547] This conduct constitutes an offence whether the hindering is temporary or permanent, partial or total. Hindering may occur as a result of denial of service (DoS) attacks.[548] Denial of service attacks include blocking users from legitimate access by entering wrong passwords for the correct user name to block access for that user name, or triggering a denial of service attack alert without the attack existing at all.[549] The most typical denial of service attack is the sending of unsolicited e-mail, which causes nuisance to its recipient, particularly when sent in bulk and frequently.[550]

Countries approach this conduct differently. The United Kingdom criminalises this conduct generally, prohibiting unauthorised acts with the intent to impair the operation of a computer.[551] Also, South Africa criminalises this conduct generally, proscribing intentionally interfering with data by modifying, destroying or otherwise rendering the data ineffective.[552] Additionally, South Africa outlaws the sending of unsolicited commercial e-mail if the consumer (the recipient) has told the sender to stop sending the unwanted e-mail.[553] Again, South Africa criminalises failing to provide the consumer with the identifying particulars of the provider of the consumer's personal details, upon the consumer's request.[554] In contrast, the United States specifically targets anyone knowingly transmitting a program, information, code, or command and intentionally causing damage to an unauthorised protected computer, or intentionally accessing an unauthorised protected computer and recklessly or otherwise causing damage.[555]

---

[546] See Schjolberg (note 56) 13.
[547] See ibid.
[548] See ibid.
[549] See ibid.
[550] See the Explanatory Report (note 221) para 67.
[551] See the Police and Justice Act s 36.
[552] See the ECTA s 86(2). See also 3.1.2 Chap three above.
[553] See the ECTA s 45(4). See also 3.1.5 Chap three above.
[554] See the ECTA s 45(3). See also 3.1.5 Chap three above.
[555] See 18 USC § 1030(a)(5). See also 2.1.5 Chap three above.

Like the United States, Lesotho can adopt the specific approach and criminalise the serious intentional hindering of the functioning of a computer system by inputting, transmitting, damaging, deleting, deteriorating, altering or suppressing computer data, without right. However, Lesotho will have to determine the extent to which the functioning of the system must be hindered - partially or totally, temporarily or permanently - to amount to serious harm justifying criminal sanction.[556]

Misuse of devices

Lesotho must criminalise the misuse of devices for committing illegal access or interception, or data and system interference.[557] This provision aims to criminalise producing, selling, obtaining, possessing, distributing or supplying a device (such as a computer virus or other malicious programs, or a computer password, access code or similar data) intentionally for use in committing a cybercrime.[558]

Computer viruses and malicious programs are basic tools for committing cybercrimes.[559] Computer viruses dangerously and economically threaten cyberspace and all netizens.[560] This provision covers devices designed or adapted primarily for committing cybercrimes.[561] It does not cover devices designed or adapted for legitimate use (such as tools meant for testing and protecting the security of systems).[562]

States address this conduct differently. The United States punishes trafficking in passwords or similar information through which a computer may be accessed without authorisation if the trafficking affects interstate or foreign commerce or is for the United States Government use.[563] On the other hand, the United Kingdom has recently created a furore by introducing a new offence - developing, owning, and

[556] See the Explanatory Report (note 221) para 69.
[557] See the Convention (note 166) Art 6.
[558] See the Explanatory Report (note 221) para 72.
[559] See Schjolberg (note 56) 14.
[560] See Ibid.
[561] See the Explanatory Report (note 221) para 72.
[562] See the Convention (note 166) Art 6 para 2.
[563] See 18 USC § 1030(a)(6). See also 2.1.6 Chap three above.

distributing 'hacker tools' for criminal use - as this law fails to recognise 'dual-use' software that could be used both legitimately and otherwise.[564] This offence includes distributing tools that are 'likely to be used' criminally.[565] Perhaps, ultimately, the British people will realise that this provision aims to restrict the producing and distributing of 'hacker tools' for illegal purposes, and not to frustrate electronic commerce. By contrast, South Africa specifically prohibits unlawfully producing, selling offering to sell, obtaining, designing, adapting for use, distributing or possessing any device designed for use in committing a cybercrime.[566] This includes a computer program or a component designed primarily to overcome security measures protecting data or performing any act regarding a password, access code or any similar data unlawfully intending to utilise the item to contravene this provision.[567] Further, South Africa outlaws the use of any device or computer program to override security measures designed to protect data or access to data.[568]

In addressing 'misuse of devices' Lesotho must prohibit intentionally and without right producing, selling obtaining, possessing, distributing or supplying such devices, which are designed primarily for use in committing cybercrimes. However, Lesotho may require that a certain number of devices be possessed before criminal liability attaches.[569]

1.1.2 Amending old laws

Amending old laws is essential to address crimes that existing Lesotho laws are inadequate to prosecute. These are crimes that have existed long before computers but are now committed using computer networks..[570] Thus, to address the most frequently committed conventional crimes using computer networks, Lesotho must criminalise:

- Computer-related forgery
- Computer-related fraud

[564] See the Police and Justice Act s 37. See also 1.4.3 Chap three above.
[565] See the Police and Justice Act s 37(2). See also 1.4.3 Chap three above.
[566] See the ECTA s 86(3). See also Chap three at 3.1.2 above.
[567] See ibid.
[568] See the ECTA s 86(4). See also Chap three at 3.1.2 above.
[569] See the Explanatory Report (note 221) para 75.
[570] See 2.2.2 and 2.2.3 Chap one above. Already, Lesotho criminalises these traditional crimes.

- Computer-related extortion
- Child pornography
- Copyright infringement

Computer-related forgery

Lesotho must prohibit intentionally and without right inputting, altering, deleting, or suppressing computer data, resulting in inauthentic data that is intended to be considered or acted upon for legal purposes as if it were authentic, whether or not the data is directly readable and intelligible.[571] As Lesotho's forgery laws require visual readability of statements in a document and do not cover computer data, this provision will provide the equivalent to the forgery of tangible documents.[572] Computer-related forgery involves unauthorised creating or altering of stored data to acquire a different evidentiary value for legal purposes, relying on the authenticity of information in the data to deceive.[573] Manipulating computer data with evidentiary value may have the same serious implications as paper-based documents; therefore, it must be proscribed likewise.[574] Basically, this provision aims to protect the legally relevant security and reliability of computer data which may have consequences for legal relations.[575]

National response towards this conduct varies; the United States and the United Kingdom do not address it at all.[576] South Africa criminalises intentionally accessing, intercepting or interfering with data for obtaining any unlawful advantage by faking data with intent that it be considered or acted upon as if it were authentic.[577]

---

[571] See the Convention (note 166) Art 7. The unauthorised 'inputting' of correct or incorrect data corresponds to making a false document. Subsequent 'altering' (modifying, varying, partial changing), 'deleting' (removing data from a data medium) and 'suppressing' (holding back, concealing data) generally corresponds to falsifying a genuine document. See also the Explanatory Report (note 221) para 83. The term 'legal purposes' refers to legal transactions and documents which are legally relevant. Further, see the Explanatory Report (note 221) para 84.

[572] Lesotho's traditional forgery provisions are based on the common law, which is a mixture of Roman-Dutch and some English law note 12 Chap one. The common law defines forgery as unlawfully making a false document causing actual or potential prejudice to another, with intent to defraud. See Jonathan Burchell *The principles of criminal law* 3ed (2005) 826.

[573] See the Explanatory Report (note 221) para 81. See also the discussion of forgery at 2.3.2 Chap one above.

[574] See the Explanatory Report (note 221) para.81.

[575] See ibid.

[576] See Figure 1 Chap three above.

[577] South Africa criminalises computer-related fraud and forgery in one breath. See the ECTA s 87(2). See also 3.1.4 Chap three above.

In implementing this offence, Lesotho may additionally require an intent to defraud, or similar dishonest intent, before criminal liability attaches.[578]

Computer-related fraud

Lesotho must criminalise intentionally and without right causing loss of property to another, fraudulently or dishonestly intending to obtain an economic benefit for oneself or another, without right, by:

- inputting, altering, deleting or suppressing computer data; or
- interfering with the functioning of a computer system.[579]

Lesotho's traditional fraud provisions require deceiving a human being. Since deceiving a computer is quite impossible within this meaning, Lesotho needs new provisions addressing computer-related fraud.[580] Computer fraud involves manipulating a computer to obtain an economic benefit or other benefit for oneself or another or to cause loss of property.[581] The traditional elements for fraud still apply for computer-related fraud, namely:

- using incorrect or incomplete information;
- altering data or programs, or otherwise unlawfully influencing the result of computer operations;
- causing a loss of property or a risk of loss to another; and
- intending to obtain an unlawful economic gain for oneself or for another.[582]

This provision aims to criminalise any undue manipulation in data processing that intends to effect an illegal transfer of property.[583]

---

[578] See the Convention (note 166) Art 7.
[579] See the Convention (note 166) Art 8.
[580] Lesotho fraud provisions are based on the common law. See note 12 Chap one above. The common law defines fraud as unlawfully making a misrepresentation causing actual prejudice or potentially prejudicing another, with intent to defraud. See also Burchell (note 572) 833.
[581] The term 'loss of property' includes loss of money, tangibles and intangibles with an economic value. See the Explanatory Report (note 221) para 88. See also the discussion of fraud at 2.3.2 Chap one above.
[582] See Schjolberg (note 56) 15.
[583] The Explanatory Report (note 221) para 86.

Computer-related fraud is increasingly becoming a global issue with the rapid growth of the information technology.[584] It includes various categories of schemes; a typical example is stock fraud or online securities fraud.[585] Countries' perceptions towards conducts will always differ. The United Kingdom does not address computer-related fraud.[586] On the other hand, the United States criminalises knowingly accessing an unauthorised protected computer intending to defraud and obtaining anything of value (however, this fraud provision excludes cases involving less than $5,000 of computer use in a year).[587] Additionally, the United States criminalises fraud and related activities connected with access devices if the offence affects interstate or foreign commerce.[588] At the other extreme, South Africa prohibits both computer-related fraud and forgery in one breath (criminalising intentionally accessing, intercepting or interfering with data for obtaining any unlawful advantage by faking data with the intent that it be considered or acted upon as if it were authentic).[589]

Unlike South Africa or the United States, Lesotho must have a clearly defined computer-related fraud provision that is separate from forgery, and also contained in one piece of legislation to avoid confusion.

Computer-related extortion

Lesotho must proscribe the unauthorised accessing, intercepting or interfering with data or threatening to do so to intentionally extort money or other valuables by undertaking to cease such action or to restore the damage caused. Lesotho's traditional extortion provisions require subjecting a person to pressure to induce submission to the extorter's demands and do not cover computer-related extortion.[590] Computer-related extortion involves transmitting a communication that threatens to

[584] See Schjolberg (note 56) 15.
[585] See the discussion of fraud at 2.3.2 Chap one above.
[586] See Figure 1 Chap three above.
[587] See 18 USC § 1030(a)(4). See also 2.1.4 Chap three above.
[588] See 18 USC § 1029. See also 2.3 Chap three above. By having more than one piece of legislation addressing the same issue the United States creates some confusion. Further, see 2.8 Chap three above.
[589] See the ECTA Act s 87(2). See also 3.1.4 Chap three above.
[590] Lesotho's traditional extortion provisions are based on the common law. The common law definition of extortion consists of taking some patrimonial advantage from another person by intentionally and unlawfully subjecting that person to pressure to induce submitting to the taking. See Burchell (note 572) 226**.**

damage a computer, in order to obtain unlawful proprietary advantage by undertaking to cease such action or to restore the damage caused. The traditional elements for extortion still apply for computer-related extortion, namely:

- unlawfully applying pressure;
- inducing submitting to the demand; and
- intending to obtain some advantage.[591]

This provision intends to criminalise the transmission of threats to crash computer systems intentionally, in order to extort money or other valuables.

Cybercriminals use extortion as a new threat: they will crash computer systems if their demands are not met. As always, countries respond to conduct differently. The United Kingdom does not address computer-related extortion. The United States prohibits transmitting threatening communication to damage a protected computer, intentionally to extort money or other valuables.[592] Similarly, South Africa criminalises the unauthorised accessing, intercepting or interfering with data or threatening to do so for obtaining unlawful proprietary advantage by undertaking to cease such action, or to restore the damage caused.[593]

Like South Africa, Lesotho must clearly define computer-related extortion; criminalising the unlawful acts and threats to crash systems to intentionally extort an economic benefit.

Child Pornography

Lesotho must criminalise offences related to child pornography committed through a computer system by prohibiting:

- intentionally and without right producing child pornography for distributing through a computer system;

[591] See Burchell (note 572) 828-29.
[592] See 18 USC § 1030(a)(7). See also 2.1.7 Chap three above.
[593] See the ECTA s 87(1). See also 3.1.3 Chap three above.

- intentionally and without right offering or making available child pornography through a computer system;

- intentionally and without right distributing or transmitting child pornography through a computer system;

- intentionally and without right procuring child pornography for oneself or for another through a computer system; and

- intentionally and without right possessing child pornography in a computer system or on a computer-data storage medium.[594]

Lesotho does not address child pornography.[595] This provision aims to protect children by modernising the criminal law to address the use of computer systems in committing sexual offences against children.[596]

Child pornography on the Internet is ever-increasing, primarily for trading the material, and threatens to undermine children's growth by leaving irreparable harm.[597] Yet again, States address this conduct differently. The United Kingdom addresses child pornography by criminalising the taking, permitting to be taken or making, distributing or showing, possessing, publishing or causing publishing any indecent photograph or indecent pseudo-photograph of a child, including by electronic and other means capable of converting into a photograph.[598] Turning to the United States, two separate laws generally regulate this conduct: the Communications Decency Act and the Child Online Protection Act.[599] The former prohibits making or soliciting and

[594] See the Convention (note 166) Art 9.
[595] See the Sexual Offences Act 29 of 2003. This law generally regulates traditional pornography; it does not specifically address child pornography.
[596] Criminalising 'producing' child pornography is necessary for combating this crime at its origins. 'Offering' covers soliciting others to obtain child pornography, 'making available' covers placing child pornography on line for the use of others, for example, by creating child pornography websites. 'Distributing' refers to actively disseminating the material, and 'transmitting' covers sending the material through a computer system to another person. The term 'procuring for oneself or for another' means actively obtaining child pornography, for instance, by downloading it. See the Explanatory Report (note 221) para 94-97.
[597] See the discussion of obscene material/pornography at 2.3.1 Chap one above.
[598] See the Protection of Children Act ss 1 and 7. See also 1.3 Chap three above.
[599] See 47 USC § 223.

initiating to transmit child pornography intending to annoy, abuse, threaten or harass another person or knowing the recipient to be below 18 years.[600] The latter prohibits knowingly availing harmful material to minors for commercial purposes 'by means of the World Wide Web,' in interstate or foreign commerce, unless the person has restricted access by minors.[601] On the other hand, South Africa prohibits possessing, producing, procuring, accessing, and distributing child pornography, and also obliges service providers to take reasonable steps to prevent the distribution of child pornography.[602]

In respect of child pornography offences, Lesotho must address pornographic material depicting:

- a minor engaged in a sexually explicit conduct;
- a person appearing to be a minor engaged in sexually explicit conduct; and
- realistic images representing a minor engaged in a sexually explicit conduct.

Still, Lesotho may decide only to criminalise pornographic material depicting a minor engaged in a sexual explicit conduct, focusing more directly on protection against child abuse.[603] However, covering material depicting a person appearing as a minor and images representing a minor engaged in a sexually explicit conduct 'while not necessarily creating harm to the 'child' depicted in the material, as there might not be a real child, might be used to encourage or seduce children into participating in such acts, and hence form part of a subculture favouring child abuse.'[604] Moreover, for international uniformity, Lesotho must define the term 'minor' as it relates to child pornography as persons under 18 years; however, Lesotho may still require a lower age-limit for this offence, but it should not be less than 16 years.[605] Further, Lesotho may adopt a more specific approach in attaching criminal liability; for example, to impose liability only for 'knowledge and control' when transmitting or storing information. Furthermore, Lesotho may not criminalise procuring and possessing

[600] See 47 USC § 223(a)(1)(A) and (B). See also 2.5.1 Chap three above.
[601] See 47 USC § 231(a)(1). See also 2.6 Chap three above.
[602] See the Films and Publication Act ss 27 and 27A. See also 3.3 Chap three above.
[603] See the Explanatory Report (note 221) para 102. See also the Convention (note 168) Art 9(4).
[604] See the Explanatory Report (note 221) para 102.
[605] See the Convention (note 166) Art 9(3).

child pornography, but attaching criminal consequences to each participant's conduct in the chain from producing to possessing would be more effective in curtailing the production of child pornography.[606] To effectively address child pornography online, Lesotho must amend the existing law to specifically address traditional child pornography.

Copyright infringement

Lesotho must criminalise wilfully committing offences related to infringements of copyright and related rights for commercial purposes through a computer system.[607] Lesotho's copyright law does not address offences committed by electronic means.[608] Reproducing and disseminating copyrighted materials electronically is fairly easy and frequently occurs without the copyright holder's consent, hence the need for criminal sanctions.[609] This provision seeks to protect the unauthorised copying, reproducing and disseminating of copyright and related rights on computer networks.

Disseminating copyrighted works via the Internet is rapidly increasing, causing concern both to copyright holders and those working professionally with computer networks.[610] Generally, all States criminalise copyright infringement, although defining the precise manner of the infringements may vary. For instance, the United Kingdom addresses copyright infringements by prohibiting making for selling

---

[606] See the Explanatory Report (note 221) para. 98. Article 9(4) of the Convention provides that a party reserves the right not to criminalise procuring and possessing (although Lesotho is not a party to this Convention, all States are urged to join it and associating with the Convention is a good start for Lesotho).

[607] See the Convention (note 166) Art 10.

[608] See the Lesotho Copyright Order 13 of 1989. Lesotho merely criminalises copyright infringement relating to original literary, artistic and scientific works, including folklore expressions. See the Lesotho Copyright Order ss 3 and 4. As a member of the World Intellectual Property Organisation (WIPO), Lesotho also protects copyright under international conventions (the WIPO Copyright Treaty and the WIPO Performances and Phonogram Treaty, often known as the Internet Treaties), setting down international norms for preventing unauthorized access to and using creative works on the Internet or other digital networks. However, breaching such copyright would only entitle the copyright holder to a civil remedy, as Lesotho's domestic law does not criminalise the conduct. Lesotho only penalises violating rights specified in the Copyright Order. See also the WIPO Copyright Treaty available at *http://www.wipo.int/treaties/en/ip/wct/trtdocs_wo033.html* [Accessed 17 January 2007] and the WIPO Performances and Phonogram Treaty also available at *http://www.wipo.int/treaties/en/ip/wppt/trtdocs_wo034.html* [Accessed 17 January 2007]. Further, see the Lesotho Copyright Order s 37.

[609] See the Explanatory Report (note 221) para 107.

[610] See the discussion of software and other copyright infringement at 2.3.2 Chap one above. See also The World Intellectual Property Organisation 'What is copyright?'WIPO Publication No. L450CR/E. Available at *www.wipo.int* [Accessed 10 October 2006].

or hiring, selling, hiring, importing, possessing, offering for selling or hiring, publicly exhibiting or distributing, or copying copyright, including a computer program.[611] On the other hand, the United States criminalises unlawfully reproducing and distributing copyright including by electronic means.[612] Again, South Africa criminalises unlawfully importing, selling, letting, offering for selling or hiring, distributing copyright or acquiring an article relating to a computer program.[613]

Lesotho must establish the wilful committing of copyright infringements and related rights for commercial purposes on computer networks as a criminal offence. However, Lesotho may 'wish to go beyond the threshold of "commercial scale" and criminalise other types of copyright infringement as well.'[614]

1.1.3 Establishing ancillary liability and sanctions

Lesotho must establish ancillary liability and define sanctions relating to cybercrimes, addressing:

- Attempt and aiding and abetting
- Corporate liability
- Reporting requirement
- Civil rights
- Sanctions

Attempt and aiding and abetting

Lesotho must criminalise the intentional attempting and aiding and abetting of any cybercrime offence intending that an offence be committed.[615] This provision aims to

[611] See the Copyright, Designs and Patents Act s 107. See 1.4 Chap three above.
[612] See the Copyright Act 17 USC § 501-(a). See also 2.7 Chap three above.
[613] See the Copyright Act s 23.
[614] See the Explanatory Report (note 221) para 114.
[615] See the Convention (note 166) Art 11.

establish additional offences relating to attempting and aiding and abetting cybercrimes.[616]

Legal systems have varying concepts for attempt, and generally, legal systems limit the offences for which attempt will be punished. Further, countries may establish criminal liability relating to aiding and abetting differently. On the one hand, the United Kingdom does not address attempts to commit cybercrimes, but criminalises aiding and abetting cybercrimes.[617] On the other hand, the United States criminalises attempting and aiding and abetting cybercrimes.[618] Similarly, South Africa criminalises attempts to commit cybercrimes and also prohibits aiding and abetting the crimes.[619]

In attaching criminal liability for aiding and abetting, Lesotho must require the intention to commit a crime, so that no liability attaches to a person acting without the requisite intent. For example, although transmitting harmful or malicious code through the Internet requires the service provider's assistance as a conduit, a service provider without the criminal intent cannot incur liability under this provision.[620]

In criminalising all attempts to commit cybercrimes, Lesotho may find some elements of offences conceptually difficult, for instance, the elements of offering and making available child pornography. Therefore, Lesotho may criminalise attempt for offences that are conceptually easy to attempt. Alternatively, Lesotho may use her own discretion in establishing attempt.[621]

Corporate liability

Lesotho must criminalise the committing of cybercrimes by legal persons. This provision intends imposing liability on corporations, associations and similar legal persons for the criminal activities committed by a 'person who has a leading position'

[616] See the Explanatory Report (note 221) para 118.
[617] See Figure 1 Chap three above.
[618] See 18 USC § 1030(c). See also 2.1 and Figure one Chap three above, respectively.
[619] See the ECTA s 88. See also 3.1.5 Chap three above.
[620] See the Explanatory Report (note 221) para 119.
[621] See the Convention (note 166) Art 11(2) and (3). Lesotho may even opt not to criminalise attempt.

within the legal person, for the legal person's benefit.[622] For attaching liability, four conditions must be met:

- the offences Lesotho describes as cybercrimes must have been committed;
- the offence must have been committed for the legal person's benefit;
- a person in a leading position must have been committed the offence (including aiding and abetting); and
- the person in a leading person must have acted based on:
  - the legal person's power of representation;
  - an authority to take decisions on behalf of the legal person; or
  - an authority to exercise control within the legal person.[623]

Additionally, Lesotho must attach liability to a person in a leading position failing to supervise an employee or the legal person's agent, with the failure facilitating the employee's or agent's committing a cybercrime.[624] Before attaching liability, the conditions to be met are:

- the legal person's employee or agent must have committed the offence;
- the offence must have been committed for the legal person's benefit; and
- committing the offence must have been made possible by the leading person's failure to supervise the employee or agent.[625]

---

[622] See the Convention (note 166) Art 12. See also the Explanatory Report (note 221) para 123. The term 'person who has a leading position' refers to a natural person in a high position in the organization, like a director. Further, see the Explanatory Report (note 221) para 124.
[623] See the Convention (note 166) Art 12(1). See also the Explanatory Report (note 221) para 124. These pre-conditions demonstrate that the person acted within the scope of authority to engage the legal person's liability.
[624] See the Convention (note 221) Art 12(2).
[625] See the Convention (note 166) Art 12(2). Failure to supervise must be interpreted to include failure to take appropriate and reasonable measures to prevent employees or agents from committing an offence on the legal person's behalf. Such appropriate and reasonable measures could be based on factors like the business type, its size, the standards or the established business best practices, and others. See also the Explanatory Report (note 221) para 125.

States may provide for any form of corporate liability. According to the English law a person acting is not speaking or acting *for* the company. The person acts *as* the company and the mind directing the person's acts is the company's mind. Thus, if that mind is guilty that guilt is the company's guilt.[626] In the United States, to attach corporate criminal liability, the individual must be acting:

- within the scope of employment;
- partly or for the corporation's benefit; and
- intentionally imputing the corporation, perhaps resulting from the corporation's wilful blindness to illegal conduct, among other reasons.[627]

By implication, South Africa provides for corporate liability by defining a 'person' as including a public body.[628] Unlike these countries, Lesotho must expressly provide for corporate liability for committing cybercrimes. Lesotho may attach criminal, civil or administrative liability to the legal person.[629] However, such liability must not prejudice the natural person's liability for committing the offence.[630] More simply, 'corporate liability does not exclude individual liability.'[631]

Reporting requirement

Lesotho must consider enacting a reporting requirement for cybercrimes. Cybercrime victims, particularly companies, tend to hide cybercrime attacks because they fear negative publicity and lack faith in the law machinery. A reporting requirement will assist in investigating and prosecuting a greater number of cybercriminals.[632] Additionally, future cybercrime incidents may be reduced as more prosecutions are publicised.[633]

---

[626] See *Tesco Supermarkets Ltd v Nattrass* [1972] AC 153.
[627] See, for example, *United States v One Parcel of Land*, 965 F.2d 316 (7th Cir 1992).
[628] See the definition of 'person' in the ECTA s 1. The Act holds any person criminally liable for committing prohibited cybercrimes, according to the Act. See also the ECTA ss 86-88.
[629] See the Convention (note 166) Art 12(3).
[630] See the Convention (note 166) Art 12(4).
[631] See the Explanatory Report (note 221) para 127.
[632] See Jason Chang 'Computer hacking: making the case for a national reporting requirement' (April 2004) Berkman Center for Internet & Society at Harvard Law School Research Publication No. 2004-07. Available at http://papers.ssrn.com/sol3/papers.cfm?abstract_id=530825 [Accessed 9 January 2007].
[633] Ibid.

Civil rights

Lesotho must create civil rights for enforcing cybercrime violations and also grant the courts the power to make an order against a person convicted to pay compensation to any party that has suffered from the offending activity. This may provide an incentive to report cybercrime violations and to reinstate faith in the law machinery.

Sanctions

Lesotho must provide for punishing all cybercrimes. Undeniably, every State provides sanctions for cybercrimes under its criminal law; the United Kingdom, the United States and South Africa all punish cybercrimes under their respective laws.[634] According to the seriousness of the cybercrimes committed, Lesotho must adopt 'effective, proportionate and dissuasive sanctions,' including 'deprivation of liberty' for natural persons.[635] Moreover, to ensure that legal persons are held liable, Lesotho must provide 'effective, proportionate and dissuasive criminal or non-criminal sanctions or measures, which include monetary sanctions.'[636] Since this provision allows for the possibility of other sanctions or measures reflecting the seriousness of the offences, Lesotho may create a system of criminal offences and sanctions compatible with the existing national legal system.[637]

1.2 Procedural law

Lesotho must establish powers and procedures for detecting, investigating and prosecuting cybercrime. Such powers and procedures will also be used for prosecuting and collecting electronic evidence of any criminal offence. These powers and procedures are:

---

[634] See the United Kingdom law, all the United States laws and South African laws as contained in chapter three above.
[635] See the Convention (note 166) Art 13(1). See the Explanatory Report (note 221) para 128.
[636] See the Convention (note 166) Art 13(2).
[637] See the Explanatory Report (note 221) para 130 note. Lesotho may employ measures such as injunction and forfeiture.

- *Expedited preservation of stored computer data*: measures necessary for authorities to order or obtain expeditious preservation of specified stored computer data.[638]

- *Expedited preservation and partial disclosure of traffic data*: measures obliging service providers to expeditiously preserve and disclose a sufficient amount of traffic data to identify service providers and the path which transmitted the communication.[639]

- *Production order*: measures empowering authorities to order a person within the territory to submit specified computer data in that person's possession, stored in a computer system, or a computer-data storage medium; or a service provider to submit subscriber information.[640]

- *Search and seizure of stored computer data*: measures empowering authorities to search and seize stored computer data.[641]

- *Real-time collection of traffic data*: measures empowering authorities to collect or record real-time traffic data for specified communications transmitted by a computer system.[642]

- *Interception of content data*: measures empowering authorities to collect and record real time data for serious offences associated with specified communications transmitted by a computer system.[643]

- *Jurisdiction*: measures establishing jurisdiction over cybercrimes committed:
  - within the territory;
  - on board a ship flying the State's flag;
  - on board an aircraft registered under the State's law; or

[638] See the Convention (note 166) Art 16.
[639] See the Convention (note 166) Art 17.
[640] See the Convention (note 166) Art 18.
[641] See the Convention (note 166) Art 19. Lesotho can do this in the same manner as with traditional tangibles. See also Schjolberg (note 56) 16.
[642] See the Convention (note 166) Art 20.
[643] See the Convention (note 166) Art 21.

- by any national, if the offence is punishable under criminal law where it was committed or if the offence is committed outside the State's territorial jurisdiction.

Except for offences committed in the territory, Lesotho may not apply these jurisdiction rules, or may apply them only in specific cases or conditions.[644] Additionally, Lesotho must establish measures to prosecute an alleged offender in the territory if not extraditing the person to another State, solely on the person's nationality, after requesting extradition.[645] Furthermore, when more than one State claims jurisdiction for a cybercrime offence, where appropriate, Lesotho could consult with other States to determine the most appropriate jurisdiction for prosecution.[646]

1.3 Mutual legal assistance agreements

Lesotho must establish a rapid and effective system for international cooperation for the 'smooth and rapid flow of information and evidence internationally.'[647] Lesotho can establish this system by adopting the principles relating to mutual legal assistance efforts for countries to trace cybercriminals in cyberspace. These include:

- Extradition
- Voluntarily disclosing information
- Confidentiality and the limitations on using shared information
- Communications between central authorities
- Requests for preserving, accessing and disclosing stored data
- Interception of data
- Trans-border access to stored computer data, 24-hours-a-day, seven-days-a-week[648]

[644] See the Convention (note 166) Art 22(2).
[645] See the Convention (note 166) Art 22(3). This is based upon the principle of nationality, which provides that nationals of a State are obliged to comply with the domestic law even when they are outside its territory. See also the Explanatory Report (note 221) para 236.
[646] See the Convention (note 166) Art 22(5).
[647] See the Explanatory Report (note 221) para 242.
[648] See the Convention (note 166) Art 23-35.

2. Conclusion

Aided by the various international and supranational efforts on cybercrime and some national approaches on cybercrime, this chapter illustrates how Lesotho can legislate to curb cybercrime. However, Lesotho cannot fight cybercrime within the framework of domestic legislation alone. Actually, little consensus exists among nations on exactly what constitutes cybercrime.[649] Different States have different approaches and different legal systems, standards and rules; therefore, harmonisation would be complicated. Some States might even opt out of the system and pose 'as offshore havens' for cybercrime.[650] Indisputably, in the networked world, 'no island is an island'; unless jurisdictions define crimes similarly, coordinated efforts by the law enforcement agencies to fight cybercrime will almost certainly fail.[651] Consequently, all States must make a determined effort to identify the shortcomings of their own current laws, and draft and adopt a comprehensive cybercrime law. Indeed, various bodies active in combating cybercrime share a common theme, namely, the need for States to have consistent adequate laws defining the basic cybercrime offences and standardising the procedures governing investigations.[652]

[649] See Figure 1 Chap three above. Also, countries used in Chap three have shown varied definitions.
[650] See Gelbstein (note 72) 85.
[651] See McConnell International note 1.
[652] These bodies include the OECD, the COE, the UN, the EU and the G-8. See generally Chap two above.

CHAPTER FIVE: CONCLUSION

Overview

Cybercrime presents a problem that Lesotho has never before had to address, and to meet this challenge Lesotho has to review her domestic laws to determine if they are adequate to combat this 'new' crime. However, legislation alone cannot protect Lesotho against cybercrime. For laws to work properly, law enforcement must be capable of implementing the law. Additionally, private citizens must take reasonable steps to protect themselves. Certainly, as the McConnell International study notes:

> [i]f home owners failed to buy locks for their front doors, should towns solve the problem by passing more laws or hiring more police? Even where laws are adequate, firms dependent on the network must make their own information and systems secure. And where enforceable laws are months or years away, as in most countries, this responsibility is even more significant.[653]

Thus, Lesotho must educate law enforcement agencies, implement measures to alleviate this problem, and police the Internet to detect cybercrime violations. Therefore, this chapter concludes that indeed cybercrime is a 'beast,' a serious problem that needs serious attention. This study also concludes that Lesotho must educate her people about cybercrime, implement protective measures against this crime, and police the Internet.

1. The nature of the 'beast'

Undeniably, cybercrime poses a serious threat to the security of systems and networks, resulting in serious security and/or financial implications. It is committed subtly and sophisticatedly, and has become a 'weapon of choice', mostly among white

[653] McConnell International note 1.

collar criminals.[654] Also, it poses serious threats to the health and safety of citizens, particularly children affected by child pornography.[655]

Countless other activities may seriously affect the security of systems and emerge as a threat to Lesotho's security.[656] For instance, espionage or disinformation can be disruptive enough to instil fear and critical loss of confidence in the Government.[657] As a result, to suit her own purposes, Lesotho can decide on what other conduct constitutes cybercrime (the list of offences in the model law is open-ended).

Largely, the Convention on Cybercrime has shaped the model law for cybercrime legislation for Lesotho. Although Lesotho is not a member, fully associating with the Convention would be a step in the right direction with regard to combating cybercrime. Further, Lesotho would better prepare for the Convention by incorporating it into her own legislation, thus addressing her domestic issues before attempting the international. Meanwhile, Lesotho should consider signing and ratifying the Convention.[658]

The nature of cybercrime necessitates that the parameters of the future law be developed and negotiated globally, for a global consensus.[659] Previously, the United Nations negotiated and agreed upon the Law of the Seas; the same approach might answer the cybercrime problem.[660] The Law of the Seas involved lengthy negotiations, but the end justified the means.[661] Whilst still waiting, Lesotho must start:

---

[654] See Baker (note 6) at 62. See also 1.1.2 Chap one above.
[655] See the discussion of obscene material/pornography at 2.3.1 Chap one above.
[656] See 2.4 Chap one above.
[657] See the discussion of espionage at 2.3.3 and 2.4 Chap one above.
[658] See the Convention (note 166) Art 37(1). The Convention welcomes all States to accede to it, additionally the United States urges all States to join the Convention, and so ultimately Lesotho will ratify it. See the U.S.Department of State note 237.
[659] See Gelbstein (note 72) 85.
[660] See ibid. The Law of the Seas defines all aspects of uses of the seas, including civilian, commercial and military navigation, continental shelves, island and archipelago states, the concept of the 'high seas', conservation and management of species living in the seas, the common heritage of mankind, governance and many other issues. See also Gelbstein ibid 6.
[661] See ibid. The negotiations lasted almost a decade, but the consensus reached has withstood the test of time.

- Educating about cybercrime
- Implementing protective measures
- Policing the Internet

1.1 Educating about cybercrime

To investigate and protect society from cybercrime, Lesotho must train her law enforcement agencies in the use of computers; otherwise they will be powerless to act.[662] For instance, if an investigating officer does not know what an e-mail is, or even that e-mail electronic records are kept and can be found, successfully prosecuting the case may be difficult.[663] Lesotho must mandate investigating officers to have a basic level of computer literacy to be able to ask the basic questions about the crimes they will be investigating.[664] Further, Lesotho must train patrol officers to recognise a cybercrime when occurring, and to appreciate calling in an expert to deal with the situation.[665] Wrongly attending a cybercrime case may negatively affect preserving evidence, arresting the perpetrator, or successfully pursuing the prosecution of the case.[666] Moreover, Lesotho must seriously consider 'encouraging young, college-educated computer science majors to join the police force.'[667] Significantly, 'although all officers will require basic literacy in information technology, some police personnel will require in-depth training in order to effectively police the digital world.'[668]

Again, Lesotho must train presiding officers to handle cybercrime (and other related) cases. Presiding officers need to have exposure to computers; otherwise investigating officers' attempts to pursue prosecutions will be frustrated. Sadly and generally, Lesotho's members of the bench (especially the judges) are rather advanced

[662] The G-8 recommends training law enforcement and equipping them to address high-tech crimes. See 5.1 Chap two above**.**
[663] See Goodman (note 7) at 493.
[664] See ibid at 492.
[665] See ibid.
[666] See ibid.
[667] See ibid at 491.
[668] Goodman (note 7) at 493. A person performing computer forensics must have more than technical knowledge, however, an understanding of performing the work legally is crucial; relatively, the work must be done in a way that preserves the value and admissibility of the evidence. See Steven M Abrams with Philip C Weis 'Knowledge of computer forensics is becoming essential for attorneys in the information age' in Pauline C Reich (ed) *Cybercrime and Security* (2005) 2.

in age and appreciating computing skills at that age may be difficult. However, Lesotho must find a way to address this issue. Likewise, Lesotho must train prosecuting authorities to effectively handle cybercrime.

1.2 Implementing protective measures

To help alleviate cybercrime problems, Lesotho must encourage the implementation of these protective measures:

- *To become aware of the problem*: Educating the people about the dangers of cybercrime and giving it more publicity will best determine addressing the problem.[669]

- *To devise an information security strategy*: Adopting reasonable steps for protecting the security of systems and networks will avoid being easily attacked.[670]

- *To implement quick simple remedial procedures*: Timely implementation of simple solutions in set-ups (like firewalls, regularly changing passwords and the management of cookies), if not already built-in, will prevent security threats.[671]

- *To seek immediate professional help*: Immediately engaging expert assistance to check loopholes in systems, regularly, particularly for large organisations and the government, will protect the security of systems.[672]

- *To adopt international and other best practices*: Adopting international standards (like the Organisation for Economic Co-operation and Development Guidelines,

[669] See the OECD Guidelines, 2002 note 183. See also the principle of 'awareness' at 2.1 Chap two above. The majority of the people does not know about cybercrime until it hits them.
[670] See the OECD Guidelines, the principle of 'responsibility' ibid. See also 2.1 Chap two above.
[671] See the OECD Guidelines, the principle of 'response' ibid. See also 2.1 Chap two above.
[672] See the OECD Guidelines, the principles of 'response,' 'risk assessment' and 'security design and implementation' ibid. Critical infrastructures and key functions of government must engage external auditors for regular check-ups. See also 2.1 Chap two above.

the Group of Eight initiatives) and other best practices will assist in securing systems from external threats.[673]

- *To identify the gaps in national legislation*: Working closely with the industry and individuals will improve their understanding of the law for a comprehensive approach to security management. This will assist in identifying gaps in the law.[674]

- *To urge the United Nations to embark on a Law of Cyberspace*: Joining hands with other nations to urge the United Nations to embark on the Law of Cyberspace, as cybercrime poses a domestic threat that needs international cooperation to effectively address the problem.[675]

1.3 Policing the Internet

Lesotho must create special interest groups to address various information security aspects. These groups can function as 'watchdogs' 24-hours-a-day-seven-days-a-week and alert the government about security and other cybercrime violations. Also, they can be used to train others to 'enhance response capabilities.'[676]

2. Concluding remarks

- Lesotho must work together with the industry toward the common goal of controlling cybercrime and making the Internet a safe place.

- 'By increasing ethical awareness and ethical behaviour in cyberspace and by introducing and evaluating the relevance and appropriateness of legislation'

---

[673] See the OECD Guidelines, the principles of 'ethics' and 'democracy' ibid. See also 2.1 Chap above.
[674] See the OECD Guidelines, the principle of 'security management' ibid. See also 2.1 Chap two above.
[675] See the OECD Guidelines, the principle of 'reassessment' note 185. See also 2.1 Chap two above.
[676] See the G8 Principles for Protecting Critical Information Infrastructures note 312. See also the discussion of the G-8 principles at 5.1 Chap two above.

Lesotho would avoid having her citizens resort to extreme measures for the security of their systems.[677]

- By legislating on cybercrime Lesotho would be breaking new ground in the area of cybercrime as a small developing country in Africa specifically addressing spreading criminal activities in cyberspace.

- Since cybercrime penetrates the whole world, all countries should adopt a model of law that will also penetrate all countries. Thus Lesotho must urge her fellow countries to adopt cybercrime legislation.

- Indeed, the cybercrime war is fiercely raging, but the armoury is not far away, and will come soon to Lesotho if she adopts cybercrime legislation.

- Cybercrime is a true 'beast', a menace to society that Lesotho has to address to enjoy the benefits of the electronic age. Otherwise, her citizens will be unnecessarily vulnerable to cybercriminals.

- To strike a balance between guaranteeing citizens their rights and combating cybercrime, Lesotho must enact this law within the parameters of the Constitution and the fundamental national commitment to protecting human rights and freedoms.

- Cybercrime is already a difficult concept, with complex terminology. Therefore, in drafting the law, Lesotho must use simple words and prefer using the active verb rather than the passive, for clarity and accessibility.[678] Additionally, Lesotho must clearly define all the elements of the offences and the use of terms.

---

[677] See D P van der Merwe L Pretorious and A Barnard 'Cyberethics and the South African Electronic Communications and Transactions Act.' Available at *http://www.ccsr.cse.dmu.ac.uk/conferences/ethicomp/ethicomp2004/abstracts/12.html* [Accessed 20 October 2006].

[678] The drafting personnel must avoid complicating the language by unnecessarily using legal phrases and difficult words. The law has been made difficult by such approach, yet the law must be kept simple and accessible, clearly speaking to the people. Mostly, when people understand and appreciate the law they are more likely to abide by it.

Furthermore, Lesotho must have this law in one piece of legislation for easy reference and to avoid confusion.[679]

- Finally, considering that this area of law is a new concept, in drafting this law Lesotho will need an expert in Electronic Law, particularly on cybercrime related issues, and I will always be a mouse click away.[680]

[679] Newly created offences, amended traditional offences, ancillary liability, procedural law, and mutual assistance agreements must all be contained in one statute.
[680] I will be happy to oblige Lesotho by offering my skills and I will be sure to leave my contacts with the Minister of Law and Constitutional Affairs himself.

BIBLIOGRAPHY

Primary Sources

Cases

United Kingdom:

R v Gold [1987] 3 WLR 803.

R v Gold [1988] AC 1063.

R v Farquharson, Croydon Magistrates' Court, 9 December 1993.

Tesco Supermarkets Ltd v Nattrass [1972] AC 153

United States

Ashcroft v Free Speech Coalition, 535 U.S. 234 (2002).

Reno v American Civil Liberties Union, 521 U.S.844 (1997).

United States v Morris 928 F (2d Cir. 1991)

United States v One Parcel of Land, 965 F.2d 316 (7th Cir 1992).

Legislation

Constitutions

Constitution of South Africa, 1996. Available at *http://www.polity.org.za/html/govdocs/constitution/saconst.html?rebookmark=1* [Accessed 24 November 2006].

The Constitution of Lesotho, 1993. Available at *http://www.parliament.ls/documents/constitution.php* [Accessed 5 January 2007).

Statutes

Lesotho

Lesotho Copyright Order 13 of 1889.

Lesotho Telecommunications Authority Act 5 of 2000. Available at *http://www.lta.org.ls/Instruments/LTA-ACT-2000.pdf* [Accessed 17 January 2007].

Lesotho Telecommunications Authority Regulations 34 2001.

Sexual Offences Act 29 of 2003.

South Africa

Copyright Act 98 of 1978 as amended by the Copyright Amendment Act 56 of 1980, 66 of 1983, 52 of 1984, 39 of 1986, 13 of 1988, 61 of 1989, 125 of 1992, the Intellectual Property Amendment Laws 38 of 1997 and the Copyright Amendment Act 9 of 2002. Available at *http://www.gpa.co.za/pdf/legislation/Copyright%20Act.pdf* [Accessed 9 January 2007].

Electronic Communications and Transactions Act 25 of 2002. Available at *http://www.info.gov.za/gazette/acts/2002/a25-02.pdf* [Accessed 17 October 2006].

Films and Publications Act 65 of 1996 as amended by the Films and Publications Amendment Act 34 of 1999 and Act 18 of 2004. Available at *http://www.info.gov.za/acts/1996/a65-96.pdf* [Accessed 24 November 2006].

Regulation of Interception of Communications and Provision of Communications-related Information Act 70 of 2002. Available at *http://www.info.gov.za/gazette/acts/2002/a70-02.pdf* [Accessed 24 November 2006].

United Kingdom

Computer Misuse Act of 1990 (c. 18). Available at *http://www.hmso.gov.uk/acts/acts1990/Ukpga_19900018_en_1.htm* [Accessed 17 November 2006].

Copyright, Designs and Patents Act of 1988 (c. 48). Available at *http://www.opsi.gov.uk/acts/acts1988/Ukpga_19880048_en_21.htm* [Accessed 9 January 2007].

Police and Justice Act of 2006 (c. 48). Available at *http://www.opsi.gov.uk/acts/acts2006/20060048.htm* [Accessed 17 November 2006].

Protection of Children Act of 1978 (c 37) as amended by the Criminal Justice and Public Order Act of 1994 (c. 33) and the Sexual Offences Act of 2003 (c. 42). Available at *http://www.geocities.com/pca_1978/reference/pca_1978amSOA.html* [Accessed 9 January 2007].

United States

Child Online Protection Act of 1998 47 USC § 231. Available at *http://www4.law.cornell.edu/uscode/html/uscode47/usc_sec_47_00000231----000-.html* [Accessed 5 December 2006].

Communications Decency Act of 1996 47 USC § 223. Available at *http://www.cybertelecom.org/cda/cda.htm* [Accessed 5 December 2006].

Computer Fraud and Abuse Act of 1986 as amended in 1994, 1996 and in 2001 by the Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT) Act of 2001 18 USC § 1030. Available at *http://www.usdoj.gov/criminal/cybercrime/1030_new.html* [Accessed 23 November 2006].

Copyright Act of 1976, as amended, USC 17 § 506. Available at *http://www.law.cornell.edu/copyright/copyright.act.chapt5.html* [Accessed 6 December 2006].

Criminal infringement of a copyright 18 USC § 2319. Available at *http://www.usdoj.gov/criminal/cybercrime/18usc2319.htm* [Accessed 18 December 2006].

Definitions 18 USC § 2510. Available at *http://www.law.cornell.edu/uscode/18/usc_sec_18_00002510----000-.html* [Accessed 18 December 2006].

Fraud and Related Activity in Connection with Access-Devices 18 USC § 1029. *http://www4.law.cornell.edu/uscode/html/uscode18/usc_sec_18_00001029----000-.html* [Accessed 5 December 2006].

Stored Communications Act of 1986 18 USC § 2701. Available at *http://www.law.cornell.edu/uscode/18/usc_sec_18_00002701----000-.html* [Accessed 18 December 2006].

Use of Interstate Facilities to Transmit Information about a Minor 18 USC § 2425. Available at *http://www.law.cornell.edu/uscode/18/usc_sec_18_00002425----000-.htm* [Accessed 5 December 2006].

Treaties

Additional Protocol to the Convention on cybercrime, concerning the criminalisation of acts of a racist and xenophobic nature committed through computer systems CETS 189. Available at *http://conventions.coe.int/Treaty/en/Treaties/Html/189.htm* [Accessed 22 August 2006].

Council of Europe Convention on Cybercrime ETS 185. Available at *http://conventions.coe.int/Treaty/EN/Treaties/Html/185.htm* [Accessed 21 August 2006].

WIPO Copyright Treaty of 1996. Available at *http://www.wipo.int/treaties/en/ip/wct/trtdocs_wo033.html* [Accessed 17 January 2007].

WIPO Performances and Phonograms Treaty of 1996. Available at *http://www.wipo.int/treaties/en/ip/wppt/trtdocs_wo034.html* [Accessed 17 January 2007].

Secondary Sources

Books

Abrams, Steven M with Weis, Philip 'Knowledge of computer forensics is becoming essential for attorneys in the information age' in Reich, Pauline C (ed) *Cybercrime and Security* (2005) Oceana Publications, New York.

Brenner, Susan W 'Cybercrime law and policy in the United States' in Reich, Pauline C (ed) *Cybercrime and security* (2005) Oceana Publications, New York.

Burchell, Jonathan *The principles of criminal law* 3ed (2005) Juta, Lansdowne.

Buys, Reinhardt (ed) *Cyberlaw @ SA top 100 FAQs* virtualbook Eduflex.

Ferrrera, Gerald R, Lichtenstein, Stephen D, Reder, Margo E K, August, Ray and Schiano, William T *Cyberlaw: text and cases* (2001) South-Western College Publishing, Ohio.

Gelbstein, Eduardo and Kamal, Ahmad 'Information insecurity' in Reich, Pauline C (ed) *Cybercrime and Security* (2005) Oceana Publications, New York.

Hofman, Julien *A guide for South Africans doing business online* (1999) Ampersand, Cape Town.

Poulter, Sebastian *Legal dualism in Lesotho* (1979) Sesuto Book Depot, Morija.

Purugganan, Abraham A 'Philippines cybersecurity update: laws, cases &other legal issues' in Reich, Pauline C (ed) *Cybercrime and security* (2006) Oceana Publications, New York.

Reed, Chris and Angel, John *Computer law* 4ed (2000) Blackstone Press Limited, London.

Willox, Norman A 'Identity theft: authentication as a solution' in Brill, Alan E, Baldwin, Jr Fletcher N and Munro, Robert J (eds) *Cybercrime and Security* (2001) Oceana Publications, New York.

Wilson, Clay 'Computer attack and cyber terrorism: vulnerabilities and policy issues for Congress, CRS Report for Congress' in Reich, Pauline C (ed) *Cybercrime and Security* (2005) Oceana Publications, New York.

Journal Articles

Baker, Glenn D 'Trespassers will be prosecuted: computer crime in the 1990s (1993) 12 *Computer/Law Journal* 61.

Brenner, Susan W 'Toward criminal law for cyberspace: a new model of law enforcement' (2004) 30 *Rutgers Computer and Technology Law Journal* 1.

Goodman, Marc D 'Why the police don't care about computer crime' (1997) 10 *Harvard Journal of Law and Technology* 465.

Goodman, Marc D and Brenner, Susan W 'The emerging consensus on criminal conduct in cyberspace' (2002) 3 *UCLA Journal of Law and Technology*.

Raskin Xan and Schaldach-Paiva Jeannie 'Eleventh survey of white collar crime' (1996) 33 *American Criminal Law Review* 541.

Reidenberg, Joel R 'Governing networks and rule-making in cyberspace' (1996) 45 *Emory Law Journal* 911.

Schwarz, Joel Michael 'A case of identity': a gaping hole in the chain of evidence of cyber-crime (2003) 9 *Boston University Journal of Science and Technology Law* 92.

Electronic Journal

Brenner, Susan W 'Cybercrime investigation and prosecution: the role of penal and procedural law' (2001) 8 No. 2 *Murdoch University Electronic Journal of Law*. Available at *http://www.murdoch.edu.au/elaw/indices/issue/v8n2.html* [Accessed 25 January 2007].

Internet Sites

Babu, Maya 'What is cybercrime?' Available at *http://www.crime-research.org/analytics/702* [Accessed 4 October 2006].

Brenner, Susan 'Cybercrimes against persons.' Available at *http://www.cybercrimes.net/Persons/persons.html* [Accessed 6 April 2006].

Brenner, Susan 'Cybercrime against property.' Available at *http://www.cybercrimes.net/Property/property.html* [6 April 2006].

Burke, Lynn 'Love bug case dead in Manila' Wired News (21 August 2000). Available at *http://www.wired.com/news/politics/0,38342-1.html?tw=wn_story_page_next1,00.html* [Accessed 18 January 2007].

Chang, Jason 'Computer hacking: making the case for a national reporting requirement' (April 2004) Berkman Center for Internet & Society at Harvard Law School Research Publication No. 2004-07. Available at *http://papers.ssrn.com/sol3/papers.cfm?abstract_id=530825* [Accessed 9 January 2007].

Christensen, John 'The trials of K Mitnick' CNN (18 March 1999). Available at *http://www.cnn.com/SPECIALS/1999/mitnick.background/* [Accessed 17 January 2007].

Duggal, Shri Pavan 'Cyber assault & cybercrimes.' Available at *http://cyberlaws.net/cyberindia/cyberassault.htm* [Accessed 11 April 2006].

Espiner, Tom 'Lord vows to fight cybercrime laws.' Available at *http://news.zdnet.co.uk/internet/0,39020369,39271086,00.htm* [Accessed 17 November 2006].

Godwin, Mike 'Watch out: an international treaty on cybercrime sounds like a great idea, until you read the fine print.' Available at *http://cryptome.org/cycrime-godwin.htm* [Accessed 5 December 2006].

Grossman, Lev 'Attack of the love bug' (15 May 2000). Available at *http://www.time.com/time/magazine/article/0,9171,996899-6,00.html* [Accessed 16 January 2007].

Higney, Francis 'Interview with Robert Schifreen' LITF Bulletin Issue (11-13 October 2006). Available at *http://www.legalitforum.com/ipi/legalitforumv2/index.jsp?pageid=litf_bulletin_015* [Accessed 17 October 2006].

Lambert, Dave 'Clause 35 is a dog's breakfast.' Available at *http://talkpolitics.users20.donhost.co.uk/index.php?title=another_fine_mess* [Accessed 19 December 2006].

Meyer, David 'Email bomber faces retrial' ZDNET UK (11 May 2006). Available at *http://news.zdnet.co.uk/security/0,1000000189,39268334,00.htm* [Accessed 17 November 2006].

Schjolberg, Stein and Hubbard, Amanda 'Harmonizing national legal approaches on cybercrime.' Available at *http://www.itu.int/osg/spu/cybersecurity/docs/Background_Paper_Harmonizing_National_and_Legal_Approaches_on_Cybercrime.pdf* [Accessed 10 June 2006].

Van Buuren, Jelle 'European Commission wants to tackle cybercrime' (10 January 2001). Available at *http://www.heise.de/tp/english/special/enfo/4658/1.html* [Accessed 24 January 2007].

Van der Merwe, D P, Pretorious L and Barnard, A 'Cyberethics and the South African Electronic Communications and Transactions Act.' Available at *http://www.ccsr.cse.dmu.ac.uk/conferences/ethicomp/ethicomp2004/abstracts/12.html* [Accessed 20 October 2006].

Williams, Phil 'Organized crime and cybercrime: synergies, trends, and responses' (13 August 2001). Available at *http://usinfo.state.gov/journals/itgic/0801/ijge/gj07.htm* [Accessed 4 July 2006].

Miscellaneous Internet Sites (without named authors)

Center for Democracy and Technology 'Child Online Protection Act (COPA).' Available at *http://www.cdt.org/speech/copa/* [Accessed 5 December 2006].

CNN.com 'Study: Most nations' laws lag on cybercrime' (6 December 2000). Available at *http://edition.cnn.com/2000/TECH/computing/12/06/crime.tech.reut/index.html* [Accessed 11 April 2006].

Electronic Privacy Information Center 'The Council of Europe's Convention on Cybercrime' available at *http://www.epic.org/privacy/intl/ccc.html#summary* [Accessed 22 August 2006].

'G8 Communiqué Okinawa 2000' (23 July 2000). Available at *http://www.g8.utoronto.ca/summit/2000okinawa/finalcom.htm* [Accessed 5 September 2006].

McConnell International 'Cybercrime…punishment? Archaic laws threaten global information' (December 2000). Available at *http://www.mcconnellinternational.com/services/cybercrime.htm* [Accessed 20 June 2006].

Net Dialogue 'COE's Committee of Experts on Crime in Cyber-space.' Available at *http://www.netdialogue.org/background/oecccyberspace/index.shtml* [Accessed 23 January 2007].

'Okinawa Charter on Global Information Society 8'. Available at *http://www.g8.utoronto.ca/summit/2000okinawa/gis.htm* [Accessed 5 September 2006].

'Resolution 55/28 on Developments in the Field of Information Technology and Telecommunications in the Context of International Security.' Available at *http://www.amun.org/undocs/a_res_55_28.*pdf [Accessed 15 January 2007].

'Resolution 57/53 on Developments in the Field of Information Technology and Telecommunications in the Context of International Security.' Available at *http://www.itu.int/wsis/docs/background/resolutions/57-53.pdf* [Accessed 22 August 2006].

Rotten.com 'Kevin-Mitnick.' Available at *http://www.rotten.com/library/bio/hackers/kevin-mitnick/* [Accessed 15 January 2007].

SearchSecurity.com 'Distributed denial of service attack.' Available at *http://searchsecurity.techtarget.com/sDefinition/0,,sid14_gci557336,00.html* [Accessed 22 January 2007].

Social Security Online 'Identity theft.' Available at *http://www.ssa.gov/pubs/idtheft.htm* [Accessed 4 December 2006].

South African Law Reform Commission 'Discussion paper 109' (October 2005). Available at *http://www.doj.gov.za/salrc/dpapers.htm* [Accessed 8 February 2007].

South African Law Reform Commission 'Issue paper 14.' Available at *http://www.doj.gov.za/salrc/papers.htm* [Accessed 24 November 2006].

'The World Factbook.' Available at *www.cia.gov/cia/publications/factbook/geos/lt.html* [Accessed 12 January 2007].

Unity ''Hacker tools' law goes from bad to worse.' Available at *http://www.libertycentral.org.uk/content/view/403/34* [Accessed 17 November 2006].

'University of Liverpool 'Computer Misuse Act 1990.' Available at *http://www.liv.ac.uk/Regulations/Commisus.html* [Accessed 17 November 2006].

Privacy International

'Council of Europe Committee of Ministers to Member States Recommendation No. R. (95) 13 Concerning Problems of Criminal Procedural Law Connected with Information Technology.' Available at *http://www.privacy.org/pi/intl_orgs/coe/info_tech_1995.html* [Accessed 21 August 2006].

'G8 Meeting Justice and Home Affairs Ministers.' Available at *http://www.privacyinternational.org/article.shtml?cmd[347]=x-347-137754* [Accessed 26 January 2007].

'G8 meeting of the Justice Ministers begins–declaring laundry list.' Available at *http://www.privacyinternational.org/article.shtml?cmd[347]=x347-243494&als[theme]=cc%20Home%20Page* [Accessed 23 January 2007].

United States Department of Justice

'California man sentenced for recklessly damaging a protected computer owned by his former employer.' Available at *http://www.cybercrime.gov/heimSent.htm* [Accessed 23 November 2006].

'Criminal resource manual 1061 unlawful access to stored communications 18 U.S.C. § 2701.' Available at *http://www.usdoj.gov/usao/eousa/foia_reading_room/usam/tilte9/crm01061.htm* [Accessed 18 December 2006].

'Cyberstalking: a new challenge for law enforcement and industry (August 1999). Available at *http://www.usdoj.gov/criminal/cybercrime/cyberstalking.htm* [Accessed 2 February 2007].

'Frequently asked questions and answers about the Council of Europe Convention on Cybercrime.' Available at *http://usdoj.gov/criminal/cybercrime/COEFAQs.htm* [Accessed 17 January 2007].

'G8 Principles for Protecting Critical Information Infrastructures.' Available at *http://www.usdoj.gov/criminal/cybercrime/g82004/G8_CIIP_principles.pdf* [Accessed 10 October 2006].

'Kevin Mitnick sentenced to nearly four years in prison; computer hacker ordered to pay restitution to victim companies whose systems were compromised' (9August 1999). Available at *http://www.usdoj.gov.criminal/cybercrime/mitnick.htm* [Accessed 17 January 2007].

'Meeting of G8 Justice and Home Affairs Ministers' (10-11 May 2004). Available at *http://www.usdoj.gov/criminal/cybercrime/g82004/index.html* [Accessed 5 September 2006].

'Meeting of G-8 Justice and Home Affairs Ministers Washington background on G8' (11 May 2004). Available at *http://www.usdoj.gov/criminal/cybercrime/g82004/g8_background.html* [Accessed 5 September 2006].

'Meeting of the Justice Ministers of the Eight' (9-10 December 1997). Available at *http://www.usdoj.gov/criminal/cybercrime/g82004/97/communique.pdf* [Accessed 5 September 2006].

Remarks of James K Robinson 'Internet as the scene of crime' International computer crime conference (29-31 May 2000). Available at *http://www.usdoj.gov/criminal/cybercrime/roboslo.htm* [Accessed 20 June 2006].

'Statement of Attorney General Alberto R Gonzales on the passage of the Cybercrime Convention' (4 August 2006). Available at *http://www.usdoj.gov/opa/pr/2006/August/06_ag_499.html* [Accessed 23 November 2006].

'The National Information Infrastructure Protection Act of 1996 legislative analysis.' Available at *http://justice.gov/criminal/cybercrime/1030_anal.html* [Accessed 23 November 2006].

'Vallejo woman charged with embezzling more than $875,035.' Available at *http://www.cybercrime.gov/sabathiaCharged.htm* [Accessed 23 November 2006].

'Woman hacks North Bay Health Care Group' at *http://www.crime-research.org/news/10.06.2004/419* [Accessed 23 November 2006].

United States Department of State

'Council of Europe Convention on Cybercrime' (29 September 2006). Available at *http://www.state.gov/r/pa/prs/ps/2006/73354.htm* [Accessed 23 November 2006].

'United States joins Council of Europe Convention on Cybercrime' (29 September 2006). Available at *http://www.state.gov/r/pa/prs/ps/2006/73353.htm* [Accessed 23 November 2006].

'The Group of 8 (G8).' Available at *http://usinfo.state.gov/ei/economic_issues/group_of_8.html* [Accessed 5 September 2006].

Council of Europe

'About the Council of Europe.' Available at *http://www.coe.int/T/e/Com/about_coe* [Accessed 21 August 2006].

'COE's Member States.' Available at *http://www.coe.int/T/E/Com/About_Coe/member_states/default.asp* [Accessed 22 August 2006].

'Council of Europe Committee of Experts on Crime in Cyberspace Final Activity Report' (25 May 2001). Available at *http://cryptome.org/cycime-final.html#DRAFT* [Accessed 21 August 2006].

'Council of Europe Committee of Ministers to Member States Recommendation No. R. (95) 13 Concerning Problems of Criminal Procedural Law Connected with Information Technology.' Available at *http://www.coe.int/t/legal_affairs/legal_co-operation/combating_economic_crime/1_standard_settings/Rec_1995_13.pdf* [Accessed 21 August 2006].

'Council of Europe Committee of Ministers Recommendation No. R. (89) 9 on Computer-Related Crime.' Available at *http://www.coe.int/t/legal_affairs/legal_co-operation/combating_economic_crime/1_standard_settings/Rec_1989_9.pdf* [Accessed 21 August 2006].

'Council of Europe Explanatory Memorandum to the Draft Convention on Cybercrime.' Available at *http://cryptome.org/cycime-final.html#DRAFT%20REPORT* [Accessed 21 August 2006].

'Council of Europe Explanatory Report to the Convention on Cybercrime (ETS 185).' Available at *http://conventions.coe.int/Treaty/en/Reports/Html/185.htm* [Accessed 23 November 2006].

'The Parliamentary Assembly–reactions and conclusions.' Available at *http://www.coe.int/T/E/Com/Files/Themes/Cybercrime/e_assparl.asp* [Accessed 21 August 2006].

European Union

Sieber, Ulrick 'Legal aspects of computer related crime information society COMCRIME study prepared under contract with the European Union (19 January 1998). Available at *http://europa.eu.int/ISPO/legal/en/comcrime/sieber.doc:* [Accessed 22 August 2006].

European Union. Available at *http://userpage.chemie.fu-berlin.de/adressen/eu.html* [Accessed 3 February 2007].

Organisation for Economic Co-operation and Development

'About OECD.' Available at *http://www.oecd.org/about/0,2337,en_2649_201185_1_1_1_1_1,00.html* [Accessed 3 August 2006].

'Marshall Plan Speech.' Available at *http://www.oecd.org/document/10/0,2340,en_201185_1876938_1_1_1_1,00html* [Accessed 3 August 2006].

'OECD Member countries.' Available at *http://www.oecd.org/document/1/0,2340,en_2649_201185_1889402_1_1_1_1,00.html* [Accessed 3 August 2006].

'Recommendation of the Council concerning guidelines for the security of information Systems 1992.' Available at *http://oecd.org/document/19/0,2340,en_2649_201185_1815059_1_1_1_1,00.html* [Accessed 3 August 2006].

'*OECD Guidelines for the security of information systems* 1992.' Available at *http://oecd.org/document/19/0,2340,en_2649_201185_1815059_1_1_1_1,00.html* [Accessed 3 August 2006].

'*OECD Guidelines for the security of information systems and networks: towards a culture of security* 2002.' Available at *http://www.oecd.org/document/42/0,2340,en_2649_201185_15582250_1_1_1_1,00.html* [Accessed 3 August 2006].

United Nations

'Charter of the United Nations -the Preamble.' Available at *http://www.un.org/aboutun/charter/index.html* [Accessed 22 August 2006].

'Eighth United Nations Congress on the Prevention of Crime and the Treatment of Offenders.' Available at *http://www.unjin.org/Documents/EighthCongress.html/#congress* [Accessed 22 August 2006].

'Eleventh United Nations Congress on Crime Prevention and Criminal Justice.' Available at *http://www.un.org/events/11thcongress/declaration.htm* [Accessed 25 January 2007].

'History of the United Nations.' Available at *http://www.un.org/aboutun/unhistory/* [Accessed 22 August 2006].

'International review of criminal policy-United Nations Manual on the prevention and control of computer-related crime.' Available at *http://www.uncjin.org/Documents/EighthCongress.html* [Accessed 3 August 2006]. Also available at *http://www.uncjin.org/8th.pdf* [Accessed 3 August 2006].

'List of Member States.' Available at *http://www.un.org/Overview/unmember.html* [Accessed 22 August 2006].

'Resolution 53/70 on Developments in the Field of Information Technology and Telecommunications in the Context of International Security.' Available at *http://www.un.org/documents/ga/res/53/ares53-70.htm* [Accessed 15 January 2007].

'Resolution 54/49, on Developments in the Field of Information Technology and Telecommunications in the Context of International Security.' Available at *http://www.un.org/documents/ga/res/54/a54r049.pdf* [Accessed 15 January 2007].

'Resolution 55/63 on Combating the criminal misuse of information technologies.' Available at *http://www.unodc.org/pdf/crime/a_res_55/res5563e.pdf* [Accessed 15 January 2007].

'Resolution 56/121 on Combating the criminal misuse of information technologies.' Available at *http://www.unodc.org.pdf/crime/a_res_56/121e.pdf* [Accessed 15 January 2007].

'Resolution 57/239- Creation of a global culture of cybersecurity.' Available at *http://daccessods.un.org/doc/UNDOC/GEN/NO2/555/22/PDF/N0255522.pdf?OpenElement* [Accessed 22 August 2006].

'Resolution 58/199-Creation of a global culture of security and the protection of critical information infrastructures.' Available at *http://daccess.ods.un.org/doc/UNDOC/GEN/NO3/506/52/PDF/N0350652.pdf?OpenElement* [Accessed 22 August 2006].

World Intellectual Property Organisation

'What is copyright?'WIPO Publication No. L450CR/E. Available at *www.wipo.int* [Accessed 10 October 2006].